MATHEMATISCHE ZEITSCHRIFT

UNTER STÄNDIGER MITWIRKUNG VON

E. KAMKE
TÜBINGEN

K. KNOPP
TÜBINGEN

R. NEVANLINNA
HELSINKI

E. SCHMIDT
BERLIN

F. K. SCHMIDT
HEIDELBERG

HERAUSGEGEBEN VON

H. WIELANDT
TÜBINGEN

WISSENSCHAFTLICHER BEIRAT

W. BLASCHKE L. FEJÉR A. E. INGHAM
H. KNESER W. MAGNUS O. PERRON
W. SÜSS H. WEYL

63. BAND, 3. HEFT

(ABGESCHLOSSEN AM 14. NOVEMBER 1955)

BERLIN · GÖTTINGEN · HEIDELBERG
SPRINGER-VERLAG
1955

Math. Z.

Die **MATHEMATISCHE ZEITSCHRIFT**

wurde im Jahre 1918 von *L. Lichtenstein* unter der Mitwirkung von *K. Knopp*, *E. Schmidt* und *I. Schur* gegründet und herausgegeben. Nach dem Tode Lichtensteins übernahm *K. Knopp* 1933 die Herausgabe. Die Schriftleitung ergänzte sich 1933 durch *E. Kamke* und *F. K. Schmidt*, 1936 durch *R. Nevanlinna* und 1950 durch *H. Wielandt*, der 1952 die Herausgabe übernahm.

Die Zeitschrift erscheint nach Maßgabe des eingehenden Materials. Der Preis des Bandes beträgt DM 96.—.

Die Mathematische Zeitschrift ist durch jede Buchhandlung zu beziehen.

Die Mathematische Zeitschrift dient der Pflege der reinen Mathematik, doch werden auch Beiträge aus den Gebieten der theoretischen Physik und Astronomie Aufnahme finden, soweit sie mathematisch von Interesse sind. Besprechungen, Aufgaben u. dgl. werden nicht zugelassen.

Es wird ausdrücklich darauf aufmerksam gemacht, daß mit der Annahme des Manuskriptes und seiner Veröffentlichung durch den Verlag das ausschließliche Verlagsrecht für alle Sprachen und Länder an den Verlag übergeht, und zwar bis zum 31. Dezember desjenigen Kalenderjahres, das auf das Jahr des Erscheinens folgt. Hieraus ergibt sich, daß grundsätzlich nur Arbeiten angenommen werden können, die vorher weder im Inland noch im Ausland veröffentlicht worden sind, und die auch nachträglich nicht anderweitig zu veröffentlichen der Autor sich verpflichtet.

Die Mitarbeiter erhalten von ihren Arbeiten 75 Sonderdrucke unentgeltlich.

Manuskriptsendungen sind zu richten an die Mitglieder der unterzeichneten Redaktion. Die Herren Mitarbeiter werden im Interesse einer raschen Drucklegung gebeten, die Arbeiten in gut lesbarer Niederschrift einzureichen. Für den Text ist, wenn irgendmöglich, Maschinenschrift, für die mathematischen Formeln jedoch nur Handschrift zu verwenden. Etwaige Abbildungen sind auf einem besonderen Blatt zu zeichnen. Die in den Formeln etwa vorkommenden griechischen oder deutschen Buchstaben (Fraktur) sowie andere der Gefahr von Verwechselungen ausgesetzte Zeichen, z. B. die Landauschen Symbole o und O, sind stets besonders (etwa mit verschiedenfarbigen Stiften) zu kennzeichnen. Die Fußnoten sind fortlaufend zu numerieren, bei Zitaten Erscheinungsjahr und Seitenzahlen anzugeben.

Wenn zu einer bereits gedruckten Arbeit eine Berichtigung nötig wird, wollen die Herren Verfasser dem Herausgeber hiervon unverzüglich Mitteilung machen. Die Berichtigungen sollen dann am Schlusse eines Bandes gesammelt aufgenommen werden.

REDAKTION DER MATHEMATISCHEN ZEITSCHRIFT:

E. Kamke, Tübingen, Frischlinstraße 27,
K. Knopp, Tübingen, Am Apfelberg 6,
R. Nevanlinna, Helsinki (Finnland), Mäntytie 5 B,
E. Schmidt, Berlin-Steglitz, Sedanstraße 8,
F. K. Schmidt, Heidelberg, Mathematisches Institut,
H. Wielandt, Tübingen, Biesingerstraße 7.

Springer-Verlag OHG — Berlin W 35, Reichpietschufer 20. — Heidelberg, Neuenheimer Landstraße 24. — Göttingen, Weender Straße 60.

---

63. Band — **Inhalt** — 3. Heft

Seite

Jacobsthal, E., Über vertauschbare Polynome 243
Keller, O.-H., Eine Bemerkung zur Ausführung der körpertheoretischen Operationen in erträglich vielen Schritten 277
Taussky, O., Unimodular integral circulants 286
Hirsch, K. A., Über lokal-nilpotente Gruppen 290
Skolem, Th., Einige Bemerkungen über die Auffindung der rationalen Punkte auf gewissen algebraischen Gebilden 295
Hahn, W., Über analytische Lösungen linearer Differential-Differenzengleichungen . 313
Grunsky, H., Eine funktionentheoretische Integralformel 320
Specht, W., Abschätzung der Wurzeln algebraischer Gleichungen. III 324
Pólya, G., On the characteristic frequencies of a symmetric membrane 331
Loewner, Ch., On totally positive matrices 338
Motzkin, Th. S., A proof of Hilbert's Nullstellensatz 341

JACOBSTHAL, E.
Math. Zeitschr. Bd. 63, S. 243—276 (1955)

Über vertauschbare Polynome.

Dem Andenken an meinen verehrten Lehrer und Freund I. SCHUR gewidmet.

Von
ERNST JACOBSTHAL.

Einleitung.

Sind $f(x)$ und $g(x)$ zwei Polynome der Grade m und n, so sind die beiden Polynome $f(g(x))$ und $g(f(x))$ beide vom Grade $m \cdot n$, aber im allgemeinen verschieden voneinander. $f(x)$ und $g(x)$ heißen *vertauschbare*[1]) Polynome, wenn

$$f(g(x)) = g(f(x)) \tag{1}$$

ist. Für das zusammengesetzte Polynom $f(g(x))$ schreiben wir abgekürzt fg. Bei der Zusammensetzung kann eine der Komponenten oder beide den Grad 0 haben. Zu den Polynomen des Grades 0, die ja Konstanten sind, wollen wir hier auch die Zahl 0 rechnen. Für die Zusammensetzung gilt das assoziative Gesetz

$$(fg)h = f(gh). \tag{2}$$

Daher kann man die „Potenzen" $f^3 = fff$, $f^1, \ldots$ definieren. Setzt man noch $ff = f^2$, $f^1 = f$, $f^0 = x$, so ist

$$f^n f^m = f^m f^n = f^{n+m}, \qquad n, m = 0, 1, 2, \ldots. \tag{3}$$

Die f^n sind die sog. „Iterierten" von f. Daß (3) auch im Falle $n = 0$ oder $m = 0$ gilt, beruht auf dem trivialen

Satz 1. *Jedes Polynom $f(x)$ ist mit $g(x) = x$ vertauschbar.*

Bei der Zusammensetzung spielt also $g(x) = x$ die Rolle der Einheit. — Die Veranlassung zu diesen Untersuchungen war eine spezielle Folge von Polynomen, die alle miteinander vertauschbar sind, und die Frage nach ihrer *Vollständigkeit*, d.h. die Frage: Gibt es außerhalb der Folge noch andere Polynome, die mit allen Elementen der Folge vertauschbar sind? Ist ein Polynom $g(x)$ gegeben, und fragt man nach allen Lösungen $f(x)$ der Gl. (1), so kennt

[1]) Über vertauschbare rationale Funktionen liegen funktionentheoretische Untersuchungen aus den zwanziger Jahren dieses Jahrhunderts vor (FATOU, JULIA, RITT). Die Literatur findet man zusammengestellt bei J. F. RITT: (1) Permutable Rational Functions. Trans. Amer. Math. Soc. **25**, 399—448 (1923). — (2) Prime and Composite Polynomials. Trans. Amer. Math. Soc. **23**, 51—66 (1922). — (3) JULIA, G.: Mémoire sur la permutabilité des fractions rationelles. Ann. École norm. supérieure **39**, 131—215 (1922). — (4) FATON, P.: Sur un groupe de substitutions algébriques. C. R. Acad. Sci. Paris **173**, 694—696 (1921).

man ja gewisse Lösungen, nämlich die Iterierten $f(x)=g^n$ von $g(x)$. Es kann sein, daß es gar keine anderen Lösungen $f(x)$ gibt; es kann aber auch trivialerweise vorkommen, daß es andere Lösungen gibt, nämlich dann, wenn $g(x)$ selbst die Iterierte eines anderen Polynoms $h(x)$ ist. Aber selbst wenn $g(x)$ nicht die Iterierte eines anderen Polynoms $h(x)$ ist, kann es vorkommen, daß die Gl. (1) Lösungen $f(x)$ besitzt, die keine Iterierten von $g(x)$ sind. Bei den Fragen der Vertauschbarkeit nehmen die Polynome ersten und zweiten Grades eine Sonderstellung ein, wie wir noch sehen werden. Außerdem spielen die Lösungen der Schröderschen Gleichung $f(x)=x$ eine gewisse Rolle. Wir wollen sie die *Eigenwerte* des Polynomes $f(x)$ nennen.

§ 1. Die Eigenwerte eines Polynoms und seiner Iterierten.

Der Begriff des Eigenwerts eines Polynoms $y=f(x)$ ist identisch mit dem Begriff des Fixpunktes der Funktionentheorie. Das Polynom $f(x)=x$ hat jede Zahl zum Eigenwert; das Polynom $f(x)=x+b$, $b\neq 0$, besitzt überhaupt keinen Eigenwert. In allen anderen Fällen besitzt ein Polynom positiven Grades n genau n Eigenwerte, die aber auch zusammenfallen können. Dann handelt es sich um mehrfache Eigenwerte.

Satz 2. *Die einzigen Konstanten, mit denen ein Polynom vertauschbar ist, sind seine Eigenwerte.*

Denn ist $f(x)$ mit einer Konstanten $g(x)=a$ vertauschbar, so ist $fg=f(a)$ und $gf=a$, also $f(a)=a$. Das Polynom $f(x)=x+b$, $b\neq 0$, ist mit keiner Konstanten vertauschbar.

Wir bezeichnen die aus $f^0=x, f^1, f^2, \ldots$ gebildete Folge mit V_f:

$$V_f=\{f^n\}_{n=0,1,2,\ldots}. \tag{4}$$

Ist der Grad von f größer als 1, so sind alle Elemente der Folge V_f voneinander verschieden. Ist der Grad m von $f(x)$ gleich 0, $f(x)$ eine Konstante b, so ist $f^1=f^2=\cdots$ und bei $f(x)=x$ ist $f^0=f^1=f^2=\cdots$. Im Falle $f(x)=x+b$, $b\neq 0$, ist $f^n=x+nb$, und alle Elemente in (4) sind voneinander verschieden. Ist schließlich $f(x)=ax+b$ mit $a\neq 1$ und $x_0=\frac{b}{1-a}$ der Eigenwert von $f(x)$, so ist $f(x)=a(x-x_0)+x_0$ und $f^n=a^n(x-x_0)+x_0$. Ist dann a keine Einheitswurzel, so sind alle Elemente in (4) voneinander verschieden und x_0 der einzige Eigenwert, den jedes f^n bei $n\geq 1$ hat. Ist aber $a\neq 1$ eine primitive r-te Einheitswurzel, so ist $f^n=f^m$ für $n\equiv m \bmod r$, die Folge (4) ist periodisch. Für $n\not\equiv 0 \bmod r$ hat f^n nur den Eigenwert x_0, und für $n\equiv 0 \bmod r$ ist $f^n\equiv x$ und hat jede Zahl zum Eigenwert.

Da für ein beliebiges Polynom $f(x)$, das ja abgesehen vom Falle $f(x)=x+b$, $b\neq 0$, stets einen Eigenwert hat, jeder Eigenwert auch Eigenwert von $f^n(x)$ ist, so verschwindet f^n-x für jede Nullstelle von $f(x)-x$. Daher ist zu erwarten, daß das Polynom $f^n(x)-x$ durch das Polynom $f(x)-x$ teilbar ist.

Man rechnet das so aus: Ist $f(x)=\sum_{\nu=0}^{m} a_\nu x^\nu$, so wird

$$f^2(x)-f(x)=\sum_{\nu=0}^{m} a_\nu\left[\left(f(x)\right)^\nu - x^\nu\right]$$
$$=\left(f(x)-x\right)\sum_{\nu=0}^{m} a_\nu \frac{\left(f(x)\right)^\nu - x^\nu}{f(x)-x}$$
$$=\left(f(x)-x\right)H_2(x),$$

worin $H_2(x)$ die letzte Summe ist und sich nach Ausrechnung gleich

$$H_2(x)=\sum_{\nu=0}^{m-1}\left(f(x)\right)^\nu \sum_{\lambda=\nu+1}^{m} a_\lambda x^{\lambda-\nu-1} \tag{5}$$

ergibt. Also wird

$$f^2(x)-x=\left(f(x)-x\right)\left(1+H_2(x)\right). \tag{5a}$$

Setzt man nun allgemein

$$f^r(x)-x=\left(f(x)-x\right)\left(1+H_r(x)\right),\qquad H_0=-1,\ H_1=0, \tag{6}$$

so ist (6) für $r=0, 1, 2$ richtig. Indem man dann in der schon für den Index r als richtig angenommenen Formel (6) x durch $f(x)$ ersetzt und (5) und (5a) benutzt, erhält man aus

$$f^{r+1}(x)-x=f^{r+1}(x)-f(x)+f(x)-x$$

nach kurzer Rechnung für die $H_r(x)$ die Rekursionsformel

$$H_{r+1}(x)=H_2(x)\left(1+H_r(f(x))\right)\qquad r\geqq 0, \tag{7}$$

so daß (6) mit den so erhaltenen H_r für alle $r\geqq 0$ richtig ist.

Ist der Grad m des Polynomes $f(x)$ größer als 1, dann wird im allgemeinen schon $f^2(x)$ außer den Eigenwerten von $f(x)$ solche Eigenwerte besitzen, die keine von $f(x)$ sind. Das Beispiel $f(x)=x^2-\frac{3}{4}$ zeigt aber, daß es vorkommen kann, daß $f^2(x)$ keine neuen Eigenwerte aufweist. Für dieses Beispiel wird nämlich

$$f(x)-x=(x+\tfrac{1}{2})(x-\tfrac{3}{2}),$$
$$f^2(x)-x=(x+\tfrac{1}{2})^3(x-\tfrac{3}{2}).$$

Von den beiden einfachen Eigenwerten von $f(x)$ ist der eine ein einfacher, der andere ein dreifacher von $f^2(x)$ geworden. Die Bedingung dafür, daß ein Eigenwert ζ von $f(x)$ ein mehrfacher ist, lautet $f'(\zeta)=1$. Für $f'(\zeta)\neq 1$ ist ζ ein einfacher Eigenwert von $f(x)$. Für einen Eigenwert ζ von $f(x)$ ergibt (5) die Gleichung

$$H_2(\zeta)=f'(\zeta). \tag{5b}$$

Daher folgt aus (7) durch Rekursion:

$$H_r(\zeta)=f'(\zeta)+\left(f'(\zeta)\right)^2+\cdots+\left(f'(\zeta)\right)^{r-1},\qquad r\geqq 2. \tag{7a}$$

Ist also ζ ein mehrfacher Eigenwert von $f(x)$, so ist wegen $f'(\zeta)=1$ nach (7a): $H_r(\zeta)=r-1$, also zeigt (6), daß jede der Iterierten f^r diesen Eigenwert genau von derselben Ordnung hat wie f selbst. Nur für einen einfachen Eigenwert ζ von $f(x)$, $f'(\zeta)\neq 1$, kann es vorkommen, daß er ein mehrfacher Eigenwert einer Iterierten f^r wird. Damit sich dies ereignet, muß nach (6) der zweite Faktor rechts für $x=\zeta$ verschwinden, also $H_r(\zeta)=-1$ sein. Da hier $f'(\zeta)\neq 1$ ist, folgt aus $H_r(\zeta)=-1$ nach (7a), daß

$$(f'(\zeta))^r=1, \quad f'(\zeta)\neq 1. \tag{7b}$$

Ist also für einen einfachen Eigenwert ζ von $f(x)$, d.h. für $f'(\zeta)\neq 1$, $f'(\zeta)$ eine r-te Einheitswurzel, so wird für die r-te Iterierte $f^r(x)$ dieses ζ ein mehrfacher Eigenwert. Dieser Eigenwert wird sogar ein mindestens dreifacher Eigenwert von $f^r(x)$. Ich will auf diesen letzten Punkt mit Rücksicht auf das oben gegebene Beispiel besonders hinweisen. Ich gebe den Beweis, ohne die Rechnungen durchzuführen. Es wird vorausgesetzt: ζ ein Eigenwert von $f(x)$, $f'(\zeta)\neq 1$, $(f'(\zeta))^r=1$. Man differenziert erst (5) und setzt dann $x=\zeta$. Das ergibt

$$H_2'(\zeta)=\tfrac{1}{2}f''(\zeta)\left(1+f'(\zeta)\right). \tag{a}$$

Dann differenziert man die Rekursionsformel (7) und setzt auch hierin $x=\zeta$. Mit Benutzung von (7a) erhält man dann, wenn man in (7) r durch λ ersetzt,

$$H'_{\lambda+1}(\zeta)=\frac{1}{2}f''(\zeta)\frac{f'(\zeta)+1}{f'(\zeta)-1}\left((f'(\zeta))^\lambda-1\right)+(f'(\zeta))^2H'_\lambda(\zeta), \quad \lambda=0,1,\ldots. \tag{b}$$

Setzt man nun

$$\frac{H'_\lambda(\zeta)}{(f'(\zeta))^{2\lambda}}=A_\lambda, \tag{c}$$

so geht (b) über in

$$A_{\lambda+1}=\frac{1}{2}f''(\zeta)\frac{f'(\zeta)+1}{f'(\zeta)-1}\left(\frac{1}{(f'(\zeta))^{\lambda+2}}-\frac{1}{(f'(\xi))^{2\lambda+2}}\right)+A_\lambda; \quad A_0=0. \tag{d}$$

Hieraus folgt durch Summation über $\lambda=0,1,\ldots,r-1$

$$A_r=\frac{1}{2}f''(\zeta)\frac{f'(\zeta)+1}{f'(\zeta)-1}\cdot\frac{1}{(f'(\zeta))^2}\cdot B_r, \tag{e}$$

worin

$$B_r=\sum_{\lambda=0}^{r-1}(f'(\zeta))^{r-\lambda}-\sum_{\lambda=0}^{r-1}(f'(\zeta))^{2(r-\lambda)}$$

ist. Für $f'(\zeta)=-1$ folgt aus (e) sofort, daß $A_r=0$ ist und für $f'(\zeta)\neq -1$ wird $(f'(\zeta))^2\neq 1$, und dann wird $B_r=0$, also auch $A_r=0$; also ergibt sich $H'_r(\zeta)=0$, und das zeigt, daß der letzte Faktor rechts in (6) ζ noch als mindestens zweifache Nullstelle besitzt, also ζ ein mindestens dreifacher Eigenwert von $f^r(x)$ ist. Wir haben also folgenden

Satz 3. *Ist $f(x)$ ein Polynom eines Grades ≥ 2, so ist jeder mehrfache Eigenwert von $f(x)$ für jedes $f^r(x)$, $r\geq 1$, ein Eigenwert von der gleichen Vielfachheit wie für $f(x)$. Ein einfacher Eigenwert ζ von $f(x)$, für den also $f'(\zeta)\neq 1$*

ist, ist dann und nur dann für eine Iterierte $f^r(x)$ ein mehrfacher Eigenwert, wenn $(f'(\zeta))^r = 1$ ist. Er ist dann sogar ein mindestens dreifacher Eigenwert von $f^r(x)$.

Aus diesem Satze folgt, daß eine Iterierte $f^r(x)$ von $f(x)$ *alle* Eigenwerte ζ von $f(x)$ in genau der gleichen Vielfachheit wie $f(x)$ selbst besitzt, wenn für jeden einfachen Eigenwert ζ von $f(x)$ stets $(f'(\zeta))^r \neq 1$ ist. Daher gibt es unendlich viele Iterierte $f^r(x)$, bei denen die Lösungen von $1 + H_r(x) = 0$ keine Eigenwerte von $f(x)$ sind, also $f^r(x)$ neue Eigenwerte hat.

Seien nun $\zeta_1, \zeta_2, \ldots, \zeta_p$ irgendwelche p verschiedenen Eigenwerte von irgendwelchen der f^n, $n \geqq 1$, der Folge (4). Sei ζ_λ ein Eigenwert von f^{n_λ}, dann hat auch jede Iterierte von f^{n_λ}, d.h. jedes $f^{r \cdot n_\lambda}$ auch den Eigenwert ζ_λ. Ist nun m das kleinste gemeinschaftliche Vielfache der p Exponenten n_λ, so ist jedes ζ_λ, $\lambda = 1, 2, \ldots, p$, Eigenwert der Iterierten f^m. Da es aber stets für ein Polynom eines Grades > 1 eine Iterierte mit neuen Eigenwerten gibt, hat ein passendes $f^{r \cdot m}$ einen Eigenwert $\zeta \neq \zeta_\lambda$, $\lambda = 1, \ldots, p$. Daher bilden die verschiedenen Eigenwerte der Polynome $f, f^2, f^3, \ldots$ eine abzählbare Folge

$$\zeta_1, \zeta_2, \zeta_3, \ldots, \tag{8}$$

wenn der Grad von $f(x)$ größer als 1 ist. Man schreibt erst alle verschiedenen Eigenwerte von $f(x)$, dann die neuen von $f^2(x)$ usw. auf, wobei es vorkommen kann, daß einige Abteilungen leer sind.

§ 2. Die regulären und die singulären Zahlen eines Polynoms.

Sei $f(x)$ ein Polynom positiven Grades m. Setzt man in der Folge (4) überall für x eine Zahl ϑ ein, so erhält man die Zahlfolge

$$V_{f(\vartheta)} = \{f^n(\vartheta)\}_{n=0,1,2\ldots} = \{\vartheta, f(\vartheta), f^2(\vartheta), \ldots\}. \tag{4a}$$

Sind alle diese Zahlen voneinander verschieden, so soll ϑ eine *reguläre Zahl* des Polynoms $f(x)$ heißen. Jede nicht reguläre Zahl soll eine *singuläre Zahl* des Polynoms genannt werden. Für eine singuläre Zahl ϑ sind also mindestens zwei Elemente der Folge (4a) einander gleich. Für $f(x) \equiv x$ ist jede Zahl singulär.

Für $f(x) = x + b$, $b \neq 0$, ist jede Zahl regulär. Das Polynom $f(x) = ax + b$, a eine von 1 verschiedene Einheitswurzel, hat nur singuläre Zahlen, da ja (4) eine periodische Folge ist. Ist aber a keine Einheitswurzel, so ist $x_0 = \frac{b}{1-a}$ die einzige singuläre Zahl des Polynoms, alle übrigen sind reguläre Zahlen. Sei nun der Grad $m > 1$. Alle Polynome in (4) sind voneinander verschieden. Eine singuläre Zahl ϑ des Polynoms $f(x)$ ist dadurch charakterisiert, daß es eine *kleinste* natürliche Zahl p gibt, für die $f^p(\vartheta)$ gleich einem $f^r(\vartheta)$ mit $r < p$ gibt. Dann sind $f^0(\vartheta) = \vartheta$, $f^1(\vartheta), \ldots, f^{p-1}(\vartheta)$ alle voneinander verschieden. Setzt man $p = r + s$, so folgt aus $f^r(\vartheta) = f^p(\vartheta)$, daß $f^{r+1}(\vartheta) = f^{p+1}(\vartheta)$, $f^{r+2}(\vartheta) = f^{p+2}(\vartheta), \ldots$ wird. Die s Zahlen

$$f^r(\vartheta), f^{r+1}(\vartheta), \ldots, f^{r+s-1}(\vartheta)$$

wiederholen sich periodisch. Vor ihnen steht die Vorperiode:

$$f^0(\vartheta) = \vartheta, f^1(\vartheta), \ldots, f^{r-1}(\vartheta),$$

die wegfällt, wenn $r = 0$ ist. Die Folge (4a) enthält nur p verschiedene Zahlen. Schreibt man die Gleichung $f^p(\vartheta) = f^r(\vartheta)$, die ϑ als singuläre Zahl des Polynomes $f(x)$ charakterisiert, in der Gestalt

$$f^s(f^r(\vartheta)) = f^r(\vartheta), \tag{9}$$

so sieht man, daß $f^r(\vartheta)$ ein Eigenwert des Polynoms $f^s(x)$ ist, also eine der Zahlen ζ_λ der Folge (8). Man bekommt umgekehrt durch Lösung irgendeiner Gleichung $f^r(x) = \zeta_\lambda$ mit jeder Lösung ϑ eine singuläre Zahl des Polynoms, denn ist ζ_λ ein Eigenwert der s-ten Iterierten, so ist wegen

$$f^r(\vartheta) = \zeta_\lambda, \quad f^s(\zeta_\lambda) = \zeta_\lambda$$
$$f^{s+r}(\vartheta) = f^s(\zeta_\lambda) = \zeta_\lambda = f^r(\vartheta),$$

also ϑ eine singuläre Zahl des Polynoms.

Hieraus folgt

Satz 4. *Die Menge der singulären Zahlen eines Polynoms des Grades $m > 1$ ist abzählbar. Man erhält diese Zahlen ϑ als Lösungen der algebraischen Gleichungen $f^r(\vartheta) = \zeta$, worin ζ jede Zahl der Folge* (8) *bedeutet. Für jedes singuläre ϑ ist die Folge* (4a) *periodisch.*

Nennt man die Anzahl p der verschiedenen Zahlen in (4a) die *Höhe* der singulären Zahl ϑ mit Bezug auf das Polynom $f(x)$, so sind die singulären Zahlen der Höhe 1 gerade die Eigenwerte von $f(x)$ selbst. Die singulären Zahlen der Höhe 2 sind die verschiedenen Lösungen der beiden Gleichungen $f^2(x) = x$, $f^2(x) = f(x)$ unter Weglassung der Eigenwerte von $f(x)$. Dabei kann die Gleichung $f^2(x) = f(x)$ durch $f(x) = \zeta$ ersetzt werden, wobei ζ einen Eigenwert von $f(x)$ bedeutet. Man kann die singulären Zahlen eines Polynoms durch Ordnen nach ihrer Höhe numerieren. Ich bemerke noch, daß für jedes gerade Polynom und für jeden seiner von Null verschiedenen Eigenwerte ζ stets $-\zeta$ eine singuläre Zahl der Höhe 2 ist, da ja dann (4a) die Form $-\zeta, \zeta, \zeta, \zeta, \ldots$ bekommt. Ganz allgemein ist für jeden Eigenwert ζ eines Polynoms $f(x)$ jede von ζ verschiedene Lösung ϑ der Gleichung $f(x) = \zeta$ aus demselben Grunde eine singuläre Zahl der Höhe 2. Ich nenne noch die ziemlich selbstverständlichen Sätze

Satz 5. *Jede reguläre (singuläre) Zahl des Polynoms $f(x)$ ist auch eine reguläre (singuläre) Zahl jeder Iterierten von $f(x)$ und umgekehrt.*

Satz 6. *Ist ϑ regulär (singulär) mit Bezug auf das Polynom $f(x)$, so ist auch jedes $f^r(\vartheta)$ regulär (singulär) mit Bezug auf $f(x)$.*

Jedes Polynom führt also zu einer Einteilung aller Zahlen in 2 Klassen S_f und R_f, die der singulären und die der regulären Zahlen, und jede Iterierte f^r, $r \geq 1$, liefert dieselbe Einteilung (Satz 5). Die Frage nach allen Polynomen, die dieselbe Einteilung wie ein gegebenes Polynom $f(x)$ liefern, wird später gestreift werden.

§ 3. Vertauschbare Polynome.

Bekannt ist

Satz 7. *Ist ein Polynom $f(x)$ sowohl mit $g(x)$ als auch mit $h(x)$ vertauschbar, so ist f auch mit gh und mit hg vertauschbar.*

Wenn g und h beide mit f vertauschbar sind, brauchen aber g und h nicht miteinander vertauschbar zu sein. Es gibt aber einige Klassen von Polynomen f, für die für je zwei mit f vertauschbare Polynome g und h auch $gh = hg$ folgt.

Definition 1. Eine Menge von Polynomen heiße eine V-Menge, wenn alle ihre Elemente miteinander vertauschbar sind. Ist die Menge speziell abzählbar und erscheint sie in der numerierten Form $f_1, f_2, \ldots$, so heiße sie eine V-Folge.

Die Folge V_f in (4) ist abgesehen von den früher erwähnten Fällen, in denen V_f periodisch war, eine V-Folge, also sicher, wenn der Grad von $f > 1$ ist.

Definition 2. Eine V-Menge (Folge) heiße *abgerundet*, wenn sie mit g und h auch gh enthält.

Ist also der Grad von f größer als 1, so ist V_f eine abgerundete V-Folge. Enthält eine abgerundete V-Folge das Polynom f, so enthält sie auch alle Elemente von V_f, abgesehen eventuell von $f^0 = x$.

Definition 3. Eine V-Menge (Folge) heiße vollständig, wenn es außerhalb der Menge (Folge) kein Polynom *positiven* Grades gibt, das mit jedem Element der Menge (Folge) vertauschbar ist.

Eine V-Menge (Folge) enthält höchstens ein Polynom 0-ten Grades, da zwei voneinander verschiedene Polynome 0-ten Grades $f(x) \equiv a$, $g(x) \equiv b \neq a$ nie miteinander vertauschbar sind. Enthält eine V-Menge (Folge) ein Polynom 0-ten Grades $g(x) \equiv a$, so ist a nach Satz 2 Eigenwert jedes Polynoms der Menge (Folge).

Satz 8. *Eine vollständige V-Menge (Folge) ist stets abgerundet.*

Beweis. Liegen g und h in der Menge, so ist gh mit jedem Element der Menge vertauschbar (Satz 7), also liegt wegen der Vollständigkeit der Menge gh in der Menge, wenn der Grad von gh größer als 0 ist. Ist aber der Grad von gh gleich 0, also gh eine Konstante a, so ist g oder h oder beide gleich der einzigen in der Menge vorkommenden Konstanten a, also liegt gh stets in der Menge, die also abgerundet ist.

Definition 4. Eine V-Folge von Polynomen positiven Grades heiße eine V-Kette, wenn in ihr Polynome *aller* positiven Grade vorkommen.

Zum Beispiel ist die Folge

$$x, x^2, x^3, \ldots$$

eine V-Kette.

Wir werden später sehen, daß eine V-Kette nie zwei Polynome gleichen Grades enthält, also jeder Grad nur einmal vertreten ist. Daraus folgt dann sofort die Vollständigkeit der Kette. Wir werden ferner zeigen, wie man alle Ketten finden kann.

Hat die Gl. (1) bei gegebenem f nur die Lösungen $g = f^r$, so ist V_f eine vollständige V-Folge, und umgekehrt folgt aus der Vollständigkeit von V_f, daß die einzigen mit f vertauschbaren Polynome die Iterierten von f sind.

Satz 9. *Die Menge M aller Polynome $x+a$ ist eine vollständige V-Menge. Sie hat die Mächtigkeit des Kontinuums.*

Beweis. Für zwei Polynome $f(x) = x+a$, $g(x) = x+b$ der Menge ist $fg = gf = x+a+b$. Also ist M eine V-Menge, die abgerundet ist. Daß M vollständig ist, folgt schon allein daraus, daß ein mit $g(x) = x+1$ vertauschbares Polynom $f(x)$ zur Menge gehört. Denn wenn $f(x)$ mit $x+1$ vertauschbar ist, so ist $f(x)$ von positivem Grad, da $x+1$ mit keiner Konstanten vertauschbar ist, und es ist $f(x+1) = f(x)+1$, also hat $f(x)$ den Grad 1,

$$f(x) = cx + d$$

$$f(x+1) = c(x+1) + d = f(x) + 1 = cx + d + 1$$

$$c = 1$$

$$f(x) = x + d.$$

Also gehört $f(x)$ zu M. M ist vollständig.

Satz 10 (Umkehrung von Satz 1). *Das einzige Polynom, das mit jedem Polynom vertauschbar ist, ist $g(x) = x$.*

Beweis. Ist $g(x)$ mit jedem Polynom vertauschbar, so ist es unter anderem mit $f(x) = x+1$ und $h(x) = 1$ vertauschbar. Aus $gf = fg$ folgt nach dem Beweise von Satz 9, daß $g(x) = x+a$ und aus $gh = hg$ oder $1+a = 1$, $a = 0$, also $g(x) = x$.

Satz 11. *Sind $f(x)$ und $g(x)$ miteinander vertauschbar und ist ζ ein Eigenwert von $g(x)$, so ist auch $f(\zeta)$ ein Eigenwert von $g(x)$. Ist ferner η eine Lösung der Gleichung $f(x) = \zeta$, so ist auch $g(\eta)$ eine Lösung dieser Gleichung.*

Beweis. Aus $g(\zeta) = \zeta$ folgt $f(\zeta) = fg(\zeta) = g(f(\zeta))$. Daher ist $f(\zeta)$ auch ein Eigenwert von $g(x)$. — Aus $f(\eta) = \zeta$ folgt $\zeta = g(\zeta) = gf(\eta) = f(g(\eta))$. Also löst $g(\eta)$ die Gleichung $f(x) = \zeta$.

Der letzte Teil werde am Beispiel $g(x) = x^2 - 2$, $f(x) = x^3 - 3x$ illustriert, die vertauschbare Polynome sind. Nehmen wir als Eigenwert von $g(x)$ etwa $\zeta = -1$, so ist die Gleichung $f(\eta) = \zeta$: $\eta^3 - 3\eta + 1 = 0$. Dann ist nach dem letzten Teil des Satzes mit jeder Lösung η auch $\eta^2 - 2$ eine Lösung. Die kubische Gleichung ist eine Normalgleichung, ohne daß eine Adjunktion nötig ist.

Sie hat drei reelle Lösungen: $\eta_1 = 0{,}35\ldots$; $\eta_2 = -0{,}87\ldots$; $\eta_3 = 1{,}53\ldots$. $\eta_2 = \eta_1^2 - 2 = g(\eta_1)$, $\eta_3 = g(\eta_2) = g^2(\eta_1)$, $\eta_1 = g(\eta_3) = g^3(\eta_1)$. Also $\eta_\lambda = g^3(\eta_\lambda)$. Es wird mit

$$\varphi(x) = f(x) + 1 = x^3 - 3x + 1:$$

$$g^3(x) - x = \varphi(x)\,(x^5 - 5x^3 - x^2 + 5x + 2)$$

$$\varphi(x^2 - 2) = \varphi(x)\,(\varphi(x) + 2).$$

Satz 5 lehrte, daß die zu einem Polynom gehörende Einteilung aller Zahlen in 2 Klassen R und S von regulären und singulären Zahlen für jede Iterierte des Polynomes die gleiche Einteilung ergibt. Das ist ein spezieller Fall von

Satz 12. *Zwei vertauschbare Polynome $f(x)$ und $g(x)$, deren Grade größer als 1 sind, bestimmen dieselbe Einteilung aller Zahlen in zwei Klassen R und S, d.h. ist ϑ eine singuläre Zahl für f, so ist ϑ auch eine singuläre Zahl des Polynomes g und umgekehrt. Daraus folgt dann das gleiche für die regulären Zahlen.*

Beweis. Wegen der Symmetrie der Voraussetzung in f und g genügt es zu zeigen: Jede singuläre Zahl von g ist auch singuläre Zahl des Polynomes f. Da $g(x)$ einen Grad >1 hat, besitzt $g(x)$ singuläre Zahlen. ϑ sei irgendeine von ihnen. Dann ist für passendes r, s, $s \geqq 1$,

$$g^r(\vartheta) = g^{r+s}(\vartheta) = g^s g^r(\vartheta),$$

also $g^r(\vartheta)$ Eigenwert von $g^s(x)$. Da f mit g vertauschbar ist, so ist auch $f^n(x)$ mit $g^s(x)$ vertauschbar, also nach Satz 11 $f^n g^r(\vartheta) = g^r f^n(\vartheta)$, auch ein Eigenwert von $g^s(x)$. Sind alle verschiedenen Eigenwerte von $g^s(x)$ etwa $x_1, \ldots, x_q$ und sind alle verschiedenen Lösungen der q Gleichungen

$$g^r(t) = x_\lambda, \qquad \lambda = 1, \ldots, q,$$

etwa $t_1, \ldots, t_m$, so ist also wegen $g^r(f^n(\vartheta)) = x_\lambda$ die Zahl $f^n(\vartheta)$ gleich einem der t_μ für jedes $n = 1, 2, 3, \ldots$. Daher besteht $V_{f(\vartheta)}$ nur aus endlich vielen verschiedenen Zahlen. ϑ ist also singuläre Zahl des Polynoms f, w. z. b. w.

Für den Fall, daß eines der Polynome oder beide linear sind, braucht der Satz nicht zu gelten. Das läßt sich aber besser übersehen, wenn man erst alle mit einem gegebenen linearen Polynom $g(x) = ax + b$ vertauschbaren Polynome bestimmt hat.

§ 4. Das lineare Polynom $g(x) = ax + b$.

Will man alle mit $g(x) = ax + b$ vertauschbaren Polynome $f(x)$ bestimmen, kann man $a = 1$ beiseite lassen (Satz 9). Die Bedingung dafür, daß ein Polynom $f(x)$ mit $g(x) = ax + b$ vertauschbar ist, lautet

(1′) $$f(ax + b) = af(x) + b,$$

wobei wir also $a \neq 1$ annehmen können.

Der Eigenwert von $g(x)$ ist

(10) $$\zeta = \frac{b}{1 - a},$$

also

(10a) $$g(x) = a(x - \zeta) + \zeta, \qquad a\zeta + b = \zeta.$$

Aus (1′) oder Satz 11 folgt für jedes mit $g(x)$ vertauschbare Polynom $f(x)$, daß $f(\zeta) = \zeta$, also $f(x)$ auch ζ zum Eigenwert hat. Setzt man nun

(11) $$x = y + \zeta, \qquad y = x - \zeta,$$

so wird

$$f(x) - \zeta = f(y + \zeta) - \zeta = h(y) \tag{11a}$$

ein Polynom in y, das $y = 0$ zum Eigenwert hat.

Daher ist

$$h(y) = y\,k(y), \tag{12}$$

worin $k(y)$ den Grad $(n-1)$ hat, wenn $f(x)$ vom Grade n ist. Indem man nun in (1′) mittels (11), (11a) die neue veränderliche y einführt und (10) und (12) benützt, erhält man die mit (1′) gleichwertige Gleichung

$$k(a\,y) = k(y). \tag{13}$$

Der Fall, in dem $f(x)$ eine Konstante ist, also $f(x) \equiv \zeta'$, $h(y) = 0$ ist, ist als trivial beiseite gelassen worden. Ist $f(x)$ linear, so ist $k(y)$ eine Konstante C,

$$h(y) = C\,y = C(x - \zeta) = f(x) - \zeta$$

$$f(x) = C(x - \zeta) + \zeta, \tag{14}$$

was für $C = 0$ den eben erwähnten Fall $f(x) \equiv \zeta$ ergibt. ζ ist auch Eigenwert jedes linearen mit $g(x)$ vertauschbaren Polynomes. Die durch (14) definierten Polynome, unter denen für $C = a$ auch $g(x)$ vorkommt, sind alle untereinander vertauschbar.

Es gilt nämlich

Satz 13. *Die Menge aller Polynome*

$$f(x) = C(x - \zeta) + \zeta$$

bildet bei gegebenem festen ζ eine abgerundete V-Menge.

Die Richtigkeit folgt unmittelbar aus den Gleichungen

$$f_1(x) = C_1(x - \zeta) + \zeta,$$
$$f_2(x) = C_2(x - \zeta) + \zeta,$$
$$f_1 f_2 = C_1 C_2 (x - \zeta) + \zeta = f_2 f_1.$$

Die durch ζ bestimmte Polynommenge M_ζ hat Kontinuummächtigkeit. Jedes Element in M_ζ hat ζ als Eigenwert, der für $C = 0$ selbst zur Menge gehört.

Sei nun der Grad von $f(x)$ größer als 1, dann lehrt der Vergleich der Koeffizienten von y^{n-1} in (13), daß

$$a^{n-1} = 1 \tag{15}$$

ist. Ist also a keine Einheitswurzel, so ist der Fall $n > 1$ unmöglich. Hieraus folgt

Satz 14. *Die Menge M_ζ des Satzes 13 ist sogar vollständig.*

Beweis. Es gibt kein Polynom eines Grades $n \geqq 2$, das mit jedem Polynom in M_ζ vertauschbar ist, denn unter den Polynomen in M_ζ kommt z.B. auch das Polynom

$$2(z - \zeta) + \zeta = 2z - \zeta$$

vor, und da 2 keine Einheitswurzel ist, so gibt es kein Polynom eines Grades $n \geqq 2$, das mit $2z - \zeta$ vertauschbar ist.

Ist aber ein Polynom $h(x)$ linear und mit auch nur einem Element $C(x-\zeta)+\zeta$, $C \neq 1$, in M_ζ vertauschbar, so ist nach Satz 11 auch $h(\zeta)$ ein Eigenwert von $C(x-\zeta)+\zeta$, d.h. $h(\zeta)=\zeta$ und dann hat $h(x)$ die Gestalt $C'(x-\zeta)+\zeta$ und liegt in M_ζ. Außerhalb M_ζ gibt es also kein Polynom positiven Grades, das mit allen Polynomen in M_ζ vertauschbar ist. Daher ist M_ζ eine vollständige V-Menge. Mit Rücksicht auf die im Anschluß an Satz 7 gemachten Bemerkungen sei hervorgehoben: Sind $f(x)$ und $h(x)$ beide mit $g(x)=ax+b$ vertauschbar, worin a keine Einheitswurzel ist, dann ist auch $f(x)$ mit $h(x)$ vertauschbar. Dies gilt auch noch für $a=1$, $b \neq 0$ (s. Satz 9).

Nun sei $a \neq 1$ eine primitive r-te Einheitswurzel, dann ist nach (15)

$$n \equiv 1 \,(r), \qquad n = 1 + \lambda r. \tag{16}$$

Wegen

$$k(y) = \sum_{\nu=0}^{n-1} b_\nu y^\nu \tag{17}$$

folgt aus (13), daß in (17) nur solche Glieder vorkommen, bei denen $\nu \equiv 0 \,(r)$ ist; es ist also $k(y)$ ein Polynom von y^r, also mit neuer Bezeichnung

$$k(y) = \sum_{h=0}^{\lambda} a_h y^{rh}. \tag{18}$$

Daher wird nach (11a) und (12)

$$f(x) = (x-\zeta) \sum_{h=0}^{\lambda} a_h (x-\zeta)^{rh} + \zeta. \tag{19}$$

Daß diese Polynome wirklich mit $g(x)=ax+b$ vertauschbar sind, rechnet man unter Benutzung von $a^r = 1$, $(r \geqq 2)$, leicht nach. Wegen der Willkürlichkeit der Koeffizienten a_h bilden die Polynome (19) eine Menge von der Mächtigkeit des Kontinuums. Wir haben also

Satz 15. *Ist $g(x)=ax+b$, worin a eine primitive r-te Einheitswurzel $(r \geqq 2)$ ist, und ist ζ der Eigenwert von $g(x)$, so ist die Gesamtheit aller mit $g(x)$ vertauschbaren Polynome $f(x)$ durch* (19) *gegeben. Für $\lambda = 0$ erhält man speziell die früher betrachteten linearen Polynome der Menge M_ζ des Satzes 13.*

§ 5. Ähnliche Polynome.

Ist ein Polynom $f(x)$ mit dem linearen Polynom $ax+b$, $a \neq 0$, vertauschbar, also

$$f(ax+b) = af(x) + b,$$

so ist

$$\frac{f(ax+b)-b}{a} = f(x).$$

Ist $f(x)$ mit $ax+b$ nicht vertauschbar, so stellt

$$\frac{f(ax+b)-b}{a} = f_1(x) \tag{20}$$

ein von $f(x)$ verschiedenes Polynom dar, das aus $f(x)$ durch eine Ähnlichkeitstransformation gewonnen wird. Die Matrix

$$M = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \tag{21}$$

definiert die lineare Transformation:

$$x = a\,x' + b.$$

Transformiert man für $y = f(x)$ kogredient

$$y = a\,y' + b,$$

so bekommt man:

$$y' = \frac{f(a\,x' + b) - b}{a} = f_1(x'). \tag{20a}$$

Bezeichnet man die ganze lineare Transformation mit

$$T = T(a, b), \tag{22}$$

so ist

$$T^{-1} = T\left(\frac{1}{a}, -\frac{b}{a}\right) \tag{22a}$$

und der Zusammenhang zwischen $f(x)$ und $f_1(x)$ schreibt sich einfach

$$f_1(x) = T^{-1} f\, T(x). \tag{23}$$

$f_1(x)$ heißt ein zu $f(x)$ ähnliches Polynom oder die T-Transformierte von $f(x)$. Dann gilt

Satz 16. *Sind $f(x)$ und $g(x)$ zwei Polynome und f_1 und g_1 ihre T-Transformierten, dann ist $f_1 g_1$ die T-Transformierte von fg.*

Denn $f_1 g_1 = T^{-1} f\, T\, g_1(x) = T^{-1} f\, T\, T^{-1} g\, T = T^{-1}(fg)\, T$. Daraus folgt sofort: Ist $fg = gf$, so ist auch $f_1 g_1 = g_1 f_1$ oder

Satz 17. *Transformiert man zwei vertauschbare Polynome $f(x)$ und $g(x)$ durch dieselbe Transformation T in die zu ihnen ähnlichen Polynome $f_1(x)$, $g_1(x)$, so ist auch f_1 und g_1 vertauschbar.*

Will man also alle Polynome $f(x)$ bestimmen, die mit einem gegebenen Polynom $g(x)$ eines Grades $\geqq 2$ vertauschbar sind, so ist es keine Einschränkung der Allgemeinheit, wenn man $g(x)$ normiert annimmt und den zweithöchsten Koeffizienten von $g(x)$ gleich 0 setzt. Dann wendet man auf $g(x)$ und das gesuchte $f(x)$ eine und dieselbe T-Transformation $T(a, b)$ an, so ist

$$g_1 = \frac{g(ax + b) - b}{a} \quad \text{auch mit} \quad f_1 = \frac{f(a\,x + b) - b}{a}$$

vertauschbar, und wenn

$$g(x) = b_0\,x^n + b_1\,x^{n-1} + \cdots + b_n$$

ist, so wird

$$g_1 = \frac{b_0(a\,x+b)^n + b_1(a\,x+b)^{n-1} + \cdots + b_n - b}{a}$$

$$= \frac{b_0 a^n x^n + (b_0 n a^{n-1} b + b_1 a^{n-1})\, x^{n-1} + \cdots + b_n - b}{a}$$

$$= b_0 a^{n-1} x^n + a^{n-2}(n\,b\,b_0 + b_1)\, x^{n-1} + \cdots .$$

Da $n \geqq 2$ ist, so geben die Gleichungen

$$b_0 a^{n-1} = 1\,, \qquad a^{n-2}(n\,b\,b_0 + b_1) = 0$$

für a und b die Werte

$$a = \sqrt[n-1]{\frac{1}{b_0}}\,, \qquad b = -\frac{1}{n}\frac{b_1}{b_0}$$

für die gewünschte Transformation. Ist $n = 2$, so ist die Bestimmung von a und b *eindeutig*.

Ist ein Polynom $g(x)$ vom Grade n gegeben, und sind seine Eigenwerte $\zeta_1, \zeta_2, \ldots, \zeta_n$, so hat das durch $T(a, b)$ erhaltene ähnliche Polynom

$$g_1(x) = \frac{g(a\,x+b) - b}{a}$$

die Eigenwerte $\frac{\zeta_\lambda - b}{a}$, $\lambda = 1, 2, \ldots, n$. Denn die Gleichung für die Eigenwerte von $g_1(x)$ lautet $g_1(x) = x$ oder

$$g(a\,x+b) = a\,x + b\,,$$

die die Lösungen $a\,x + b = \zeta_\lambda$, $x = \frac{\zeta_\lambda - b}{a} = \vartheta_\lambda$ ergibt. Ist speziell $n = 2$, und transformiert man das quadratische Polynom $g(x)$ in ein ähnliches mit demselben höchsten Koeffizienten, d.h. wählt man $a = 1$, so ist

$$\vartheta_1 = \zeta_1 - b$$
$$\vartheta_2 = \zeta_2 - b$$

und $\vartheta_1 - \vartheta_2 = \zeta_1 - \zeta_2$. Die Differenz der Eigenwerte ist also invariant gegenüber einer solchen Transformation.

§ 6. Die Polynome

$$\boldsymbol{g(x) = b_0 x^n + b_1 x^{n-2} + \ldots + b_n\,, \qquad n \geqq 2 \qquad b_0 \neq 0.}$$

Über die Menge M der Polynome $f(x)$, die mit dem gegebenen Polynom $g(x)$ der Überschrift vertauschbar sind, gilt

Satz 18. *Ist $g(x)$ ein Polynom eines Grades $n \geqq 2$, so bilden alle mit ihm vertauschbaren Polynome $f(x)$ eine abzählbare Menge.*

Dieser Satz ist eine unmittelbare Folge von

Satz 19. *Ist m eine gegebene Gradzahl $\geqq 0$, so gibt es für $m=0$ höchstens n Polynome $f(x)$ des Grades $m=0$, die mit $g(x)$ vertauschbar sind. Für $m \geqq 1$ gibt es höchstens $(n-1)$ Polynome $f(x)$ des Grades m, die mit $g(x)$ vertauschbar sind.*

Beweis. Ist der Grad eines mit $g(x)$ vertauschbaren Polynomes $f(x)$ gleich Null, so ist $f(x)$ eine Konstante, die nach Satz 2 ein Eigenwert von $g(x)$ ist. Und da es höchstens n verschiedene solche gibt, ist der Satz im Falle $m=0$ richtig. — Sei nun $m \geqq 1$. Wir betrachten vorweg den Fall $m=1$, in dem $f(x)=a_0 x+a_1$, $a_0 \neq 0$, sein soll. Die Vertauschbarkeitsbedingung lautet: $fg=gf$. Nun ist:

$$fg = a_0 g(x) + a_1 = a_0 \sum_{\nu=0}^{n} b_\nu x^{n-\nu} + a_1$$

$$gf = g(a_0 x + a_1) = \sum_{\nu=0}^{n} b_\nu (a_0 x + a_1)^{n-\nu}.$$

Der Vergleich der Koeffizienten von x^n und x^{n-1} in beiden Ausdrücken gibt

$$b_0 a_0^n = a_0 b_0, \qquad a_0^{n-1} = 1$$
$$b_0 n a_0^{n-1} a_1 + b_1 a_0^{n-1} = a_0 b_1$$
$$b_0 n a_1 = b_1 (a_0 - 1)$$
$$a_1 = \frac{b_1 (a_0 - 1)}{n b_0}.$$

a_0 ist $(n-1)$-deutig bestimmt, und zu jedem dieser $(n-1)$ Werte a_0 ist a_1 eindeutig bestimmt. Ob mit den so gefundenen Werten von a_0, a_1 die niederen Koeffizienten der Vertauschbarkeitsgleichung links und rechts übereinstimmen, ist eine offene Frage, jedenfalls kann es nicht mehr als $(n-1)$ Polynome ersten Grades geben, die mit $g(x)$ vertauschbar sind. Da der Eigenwert des Polynoms $f(x)=a_0 x+a_1$, durch

$$\zeta = \frac{a_1}{1-a_0} = -\frac{b_1}{n b_0}$$

gegeben ist, ist das gefundene $f(x)$ nur unter gewissen Bedingungen zwischen den b_ν mit $g(x)$ vertauschbar, die aus § 4 zu entnehmen sind. — Sei nun der Grad m von $f(x)$ größer als 1. Es sei

$$f(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_m; \qquad m \geqq 2;\ a_0 \neq 0. \tag{24}$$

Die Frage ist die Bestimmung der $(m+1)$ Koeffizienten $a_0, a_1, \ldots, a_m$ mit Hilfe der Gl. (1). Da der Grad in (1) auf beiden Seiten gleich mn ist, sind im ganzen $(mn+1)$ Gleichungen von den $(m+1)$ Unbekannten a_ν zu erfüllen, also mehr Gleichungen als Unbekannte zur Verfügung stehen; es wird also im allgemeinen gar keine Lösung geben. Wir müssen zeigen, daß es, wenn die Gleichungen lösbar sind, höchstens $(n-1)$ Lösungen bei gegebenem m gibt. Die Gl. (1) lautet hier

$$\sum_{\lambda=0}^{m} a_\lambda (g(x))^{m-\lambda} = \sum_{\lambda=0}^{n} b_\lambda (f(x))^{n-\lambda}. \tag{1*}$$

Um die Koeffizientenvergleichung durchführen zu können, muß man alle Potenzen $(f(x))^p$, $(g(x))^p$ nach Potenzen von x entwickeln. Der polynomische Satz ergibt:

$$(25)\quad \begin{cases} (f(x))^p = \displaystyle\sum_{\lambda_0+\lambda_1+\cdots+\lambda_m=p} \frac{p!}{\lambda_0!\,\lambda_1!\ldots\lambda_m!}\, a_0^{\lambda_0} x^{m\lambda_0} a_2^{\lambda_1} x^{(m-1)\lambda_1} \ldots a_m^{\lambda_m} x^{(m-m)\lambda_m} \\ \quad = \displaystyle\sum_{\lambda_0+\lambda_1+\cdots+\lambda_m=p} \frac{p!}{\lambda_0!\,\lambda_1!\ldots\lambda_m!}\, a_0^{\lambda_0} a_1^{\lambda_1} \ldots a_m^{\lambda_m} x^{mp-1\lambda_1-\cdots-m\lambda_m}. \end{cases}$$

Daher wird der Koeffizient $A_{p,k}$ von x^k in $(f(x))^p$

$$(26)\quad A_{p,k} = \sum_{\substack{\lambda_0+\lambda_1+\cdots+\lambda_m=p \\ 1\cdot\lambda_1+2\lambda_2+\cdots+m\lambda_m=mp-k}} \frac{p!}{\lambda_0!\,\lambda_1!\ldots\lambda_m!}\, a_0^{\lambda_0} a_1^{\lambda_1} \ldots a_m^{\lambda_m}, \qquad k=0,1,2,\ldots,mp.$$

Entsprechend wird der Koeffizient von x^k in $(g(x))^p$

$$(27)\quad B_{p,k} = \sum_{\substack{\lambda_0+\lambda_1+\cdots+\lambda_n=p \\ 1\cdot\lambda_1+2\lambda_2+\cdots+n\lambda_n=np-k}} \frac{p!}{\lambda_0!\,\lambda_1!\ldots\lambda_n!}\, b_0^{\lambda_0} b_1^{\lambda_1} \ldots b_n^{\lambda_n}, \qquad k=0,1,2,\ldots,np.$$

Der Vergleich der Koeffizienten von x^{mn} in (1*) ergibt

$$(28)\quad a_0 b_0^m = b_0 a_0^n$$

oder

$$(28_1)\quad a_0^{n-1} = b_0^{m-1}.$$

Hierdurch ist der höchste Koeffizient a_0 von $f(x)$ $(n-1)$-deutig bestimmt. Wenn die weiteren Koeffizienten $a_1, a_2, \ldots, a_m$ sich rekursiv durch lineare Gleichungen bestimmen lassen, falls man einen der gefundenen $(n-1)$ Werte a_0 zugrunde legt, dann ist damit gezeigt, daß es höchstens $(n-1)$ Polynome $f(x)$ des Grades m geben kann, die (1*) befriedigen. Nun vergleichen wir in (1*) die Koeffizienten von x^{mn-1} auf beiden Seiten. Da m und n beide >1 sind, kommt diese Potenz links nur in $a_0(g(x))^m$ und rechts nur in $b_0(f(x))^n$ vor. Da die Koeffizienten von x^{mn-1} aus (27) und (26) zu entnehmen sind, gibt der Vergleich

$$a_0 B_{m,mn-1} = b_0 A_{n,mn-1}$$

oder

$$a_0 \sum_{\substack{\lambda_0+\lambda_1+\cdots+\lambda_n=m \\ 1\cdot\lambda_1+2\lambda_2+\cdots+n\lambda_n=1}} \frac{m!}{\lambda_0!\,\lambda_1!\ldots\lambda_n!}\, b_0^{\lambda_0} b_1^{\lambda_1} \ldots b_n^{\lambda_n} = b_0 \sum_{\substack{\lambda_0+\lambda_1+\cdots+\lambda_m=n \\ 1\cdot\lambda_1+2\lambda_2+\cdots+m\lambda_m=1}} \frac{n!}{\lambda_0!\,\lambda_1!\ldots\lambda_m!}\, a_0^{\lambda_0} a_1^{\lambda_1} \ldots a_m^{\lambda_m}.$$

Dies reduziert sich wegen der unter den Summen stehenden Relationen zwischen den Summationsbuchstaben auf

$$a_0 m b_0^{m-1} b_1 = b_0 n a_0^{n-1} a_1 = b_0 n b_0^{m-1} a_1,$$

wenn man (28_1) benutzt. Daraus folgt

$$(29)\quad a_1 = \frac{m}{n}\,\frac{a_0 b_1}{b_0},$$

so daß zu jedem der $(n-1)$ erhaltenen Werte a_0 der nächste Koeffizient a_1 eindeutig bestimmt ist.

Nehmen wir nun an, wir hätten schon mit Benutzung der gefundenen Werte a_0, a_1 durch Vergleich der Koeffizienten von x^{mn-2} den nächsten Koeffizienten a_2 eindeutig gefunden und weiter durch Vergleich der Koeffizienten von

$$x^{mn-3}, x^{mn-4}, \ldots, x^{mn-q}$$

in (1*) die Koeffizienten

$$a_3, a_4, \ldots, a_q, \qquad q \leqq m-1,$$

eindeutig errechnet, so daß wir also $a_0, a_1, \ldots, a_q$ als schon bekannt ansehen können. Wenn sich dann auch a_{q+1} durch den Vergleich der Koeffizienten von

$$x^{mn-q-1}$$

in (1*) eindeutig ergibt, dann folgt durch Induktion, daß zu jedem der $(n-1)$ Werte a_0, die sich aus (28_1) ergeben, $a_1, a_2, \ldots, a_m$ eindeutig bestimmt sind, es also höchstens $(n-1)$ Polynome $f(x)$ des Grades m geben kann, die mit $g(x)$ vertauschbar sind. Wir haben also zu zeigen, daß der Vergleich der Koeffizienten von x^{mn-q-1} in (1*) wirklich auf eine Gleichung ersten Grades für a_{q+1} führt.

Wegen $q \leqq m-1$ ist $-(q+1) \geqq -m$ und

$$mn-(q+1) \geqq mn-m = m(n-1).$$

Gilt hier das Zeichen $>$, was für $q < m-1$ der Fall ist, dann kommen Glieder mit dem Exponenten $mn-(q+1)$ auf der rechten Seite in (1*) nur in $b_0(f(x))^n$ vor, da ja das nächste Glied nur noch einen Grad $m(n-1) < mn-(q+1)$ hat. Nur für $q = m-1$ liefert dieses nächste Glied noch einen Beitrag mit dem Exponenten $mn-(q+1) = m(n-1)$, nämlich das Glied

$$b_1 a_0^{n-1} x^{m(n-1)},$$

das aber a_{q+1} nicht enthält. Das gesuchte a_{q+1} kommt also auf der rechten Seite von (1*) nur in den Gliedern vor, die von $b_0(f(x))^n$ stammen. In diesem Ausdruck wird der Koeffizient von $x^{mn-(q+1)}$ gleich

$$b_0 A_{n,mn-(q+1)} = b_0 \sum_{\substack{\lambda_0+\lambda_1+\cdots+\lambda_m=n \\ 1\cdot\lambda_1+2\lambda_2+\cdots+m\lambda_m=q+1}} \frac{n!}{\lambda_0!\,\lambda_1!\ldots\lambda_m!}\, a_0^{\lambda_0} a_1^{\lambda_1} \ldots a_m^{\lambda_m}.$$

Da nun wegen der Relationen zwischen den λ_ϱ

$$\varrho\,\lambda_\varrho \leqq q+1, \qquad \lambda_\varrho \leqq \frac{q+1}{\varrho}$$

ist, so ist für $\varrho > q+1$ sicher $\lambda_\varrho = 0$. Daher reduziert sich die letzte Formel auf

$$b_0 A_{n,mn-(q+1)} = b_0 \sum_{\substack{\lambda_0+\lambda_1+\cdots+\lambda_{q+1}=n \\ 1\cdot\lambda_1+2\lambda_2+\cdots+(q+1)\lambda_{q+1}=q+1}} \frac{n!}{\lambda_0!\,\lambda_1!\ldots\lambda_{q+1}!}\, a_0^{\lambda_0} a_1^{\lambda_1} \ldots a_{q+1}^{\lambda_{q+1}}.$$

Es tritt also nur ein Glied in der Summe auf, das a_{q+1} enthält, und zwar in der ersten Potenz, nämlich für

$$\lambda_{q+1} = 1, \quad \lambda_1 = \lambda_2 = \cdots = \lambda_q = 0, \quad \lambda_0 = n - 1.$$

Alle anderen noch auftretenden Glieder der Summe entstehen nur für $\lambda_{q+1} = 0$, d.h. sie enthalten a_{q+1} nicht.

Der Koeffizient von x^{mn-q-1} rechts in (1*) wird also

$$b_0 \left[n\, a_0^{n-1} a_{q+1} + \sum_{\substack{\lambda_0 + \lambda_1 + \cdots + \lambda_q = n \\ 1 \cdot \lambda_1 + 2 \lambda_2 + \cdots + q \lambda_q = q+1}} \frac{n!}{\lambda_0!\, \lambda_1! \ldots \lambda_q!}\, a_0^{\lambda_0} a_1^{\lambda_1} \ldots a_q^{\lambda_q} \right],$$

wozu noch im Falle $q = m - 1$ das Glied

$$b_1 a_0^{n-1}$$

zuzufügen ist.

Auf der linken Seite von (1*) hat das Glied

$$a_\varrho (g(x))^{m-\varrho} = a_\varrho (b_0 x^n + \cdots + b_n)^{m-\varrho}$$

den Grad $n(m-\varrho)$ und dieser ist $\geq mn - (q+1)$ nur für

$$\varrho\, n \leq q + 1;$$

wegen $n \geq 2$ folgt, daß dies nur der Fall ist für

$$\varrho \leq \frac{q+1}{2} \leq q,$$

da ja $q \geq 1$ ist. Der Koeffizient von x^{mn-q-1} auf der linken Seite von (1*), der ja in den a_λ linear ist, enthält also höchstens die schon bekannten Koeffizienten

$$a_0, a_1, \ldots, a_q.$$

Daher bekommen wir wirklich durch Vergleich der Koeffizienten von $x^{mn-(q+1)}$ in (1*) eine in a_{q+1} lineare Gleichung, die a_{q+1} eindeutig bestimmt, so daß der Satz bewiesen ist[2]).

Speziell für $n = 2$ folgt aus diesem Satze

Satz 20. *Ist $g(x)$ ein Polynom des Grades 2, so gibt es höchstens ein Polynom $f(x)$ eines gegebenen positiven Grades m, das mit $g(x)$ vertauschbar ist.*

Und hieraus folgt weiter

Satz 21. *Sind $f_1(x)$ und $f_2(x)$ zwei Polynome positiven Grades, die beide mit einem Polynom $g(x)$ des Grades 2 vertauschbar sind, so ist $f_1(x)$ auch mit $f_2(x)$ vertauschbar.*

[2]) Man kann mit Hilfe des zum Beweise von Satz 19 benutzten Induktionsverfahrens zeigen: Ist $g(x)$ ein gerades oder ungerades Polynom eines Grades $n \geq 2$, so ist jedes mit $g(x)$ vertauschbare Polynom $f(x)$ entweder ein gerades oder ein ungerades Polynom. Für den Fall, daß $g(x)$ ein gerades Polynom ist, läßt sich die Gleichung $f(-x) = \pm f(x)$ leicht direkt aus $fg = gf$ ableiten. Bei ungeradem n dagegen versagt diese Schlußweise, weil der Satz im Falle $n = 1$, $g(x) = ax$, falsch ist. Mit $g(x) = x$ ist jedes Polynom vertauschbar; mit $g(x) = \omega x$, $\omega^3 = 1$, $\omega \neq 1$, ist $f(x) = x + x^4$ vertauschbar.

Beweis. Da $f_1 f_2$ und $f_2 f_1$ beide nach Satz 7 in § 3 ebenfalls mit $g(x)$ vertauschbar sind und $f_1 f_2$ und $f_2 f_1$ gleichen positiven Grad haben, so ist nach Satz 20: $f_1 f_2 = f_2 f_1$.

Als Illustration zu Satz 19 sei erwähnt:

Ist $g(x) = x^n$, $n \geqq 2$, so gibt es genau $(n-1)$ Polynome eines gegebenen positiven Grades m, die mit x^n vertauschbar sind. Es sind das nämlich die $(n-1)$ Polynome $C x^m$, worin C jede der Einheitswurzeln bedeutet, die durch $C^{n-1} = 1$ gegeben sind.

Aus Satz 20 folgt noch für die in § 3, Definition 4, erklärten V-Ketten

Satz 22. *Jede V-Kette enthält genau ein Polynom m-ten Grades, $m = 1, 2, 3 \ldots$ und ist stets vollständig.*

Beweis. Da eine solche Kette ein Polynom $g(x)$ des Grades 2 enthält und es zu jedem Grade $m \geqq 1$ höchstens ein Polynom $f(x)$ des Grades m gibt, das mit $g(x)$ vertauschbar ist, die Kette aber laut Definition Polynome aller positiven Grade enthält, so enthält die Kette für jeden positiven Grad nur ein Polynom dieses Grades, und außerhalb der Kette existiert kein anderes Polynom dieses Grades, das mit $g(x)$ vertauschbar ist. Also ist die Kette vollständig. So ist die früher in § 3 genannte Folge

$$x, x^2, x^3, \ldots$$

eine vollständige V-Kette.

Genau so ergibt sich aus Satz 20 und 21

Satz 23. *Kommen in einer Folge von Polynomen positiven Grades alle Gradzahlen $m = 1, 2, 3, \ldots$ vor, und sind alle Polynome der Folge mit einem und demselben Polynom $g(x)$ zweiten Grades vertauschbar, so gehört $g(x)$ zur Folge, und die Folge ist eine V-Kette, enthält also zu jedem Grade genau einen Vertreter.*

§ 7. Die Konstruktion aller V-Ketten.

Hat man nach Definition 4 in § 3 eine V-Kette, so enthält sie nach Satz 22 zu jeder Gradzahl $m \geqq 1$ genau *einen* Vertreter und ist eine vollständige V-Folge (Definition 3 in § 3). Bezeichnet man das Element m-ten Grades der Kette mit $F_m(x)$, so ist also die Kette

$$F_1, F_2, F_3, \ldots,$$

wobei $F_1(x) \equiv x$ ist.

Für den Fall, daß alle $F_\lambda(x)$ einen gemeinsamen Eigenwert α haben, kann man die Kette durch Zufügung von $F_0(x) = \alpha$ zu einer *erweiterten Kette* machen, da ja $F_\lambda F_0 = F_0 F_\lambda = \alpha$ ist. So entstehen aus der Kette

(I) $$x, x^2, x^3, \ldots,$$

da alle Elemente in (I) sowohl 0 als auch 1 als Eigenwert besitzen, die erweiterten Ketten

(I') $$\begin{cases} 1, x, x^2, \ldots \\ 0, x, x^2, \ldots. \end{cases}$$

Transformiert man jedes F_n in einer Kette durch ein und dieselbe T-Transformation, so bilden die Polynome $T^{-1}F_nT(x)$ ebenfalls eine Kette, die zur ursprünglichen ähnlich ist. Alle zu einer gegebenen Kette ähnlichen V-Ketten sind untereinander ähnlich. Tut man alle zueinander ähnlichen V-Ketten in eine Klasse, so kann man die Frage stellen: Wie viele Klassen gibt es? Die Frage beantwortet

Satz 24. *Die Anzahl der Klassen ähnlicher V-Ketten ist gleich* 2. [Für erweiterte V-Ketten ist wegen (I') die Anzahl gleich 3.]

Beweis. Jede V-Kette enthält ein einziges Polynom zweiten Grades. Es gibt nach den im Anschluß an Satz 17 in § 5 gemachten Bemerkungen eine *einzige* T-Transformation, die dieses quadratische Polynom in ein reines Polynom x^2+b transformiert. Daher gibt es in jeder Klasse ähnlicher V-Ketten eine *einzige* Kette, in der das quadratische Polynom ein reines Polynom ist. Diese Kette soll die *Grundkette* der Klasse heißen. (I) ist die Grundkette der zu (I) gehörenden Klasse. Wir zeigen nun einfach: Es gibt nur zwei Grundketten. Damit ist dann der Satz bewiesen.

Es liege also eine Grundkette vor, in der das quadratische Polynom

$$g(x) = x^2 + b \tag{30}$$

ist. Die Grundkette enthält ein Polynom dritten Grades

$$f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3. \tag{31}$$

Wir haben wegen der Vertauschbarkeit von $f(x)$ mit $g(x)$ die Gleichung

$$f(x^2+b) = (f(x))^2 + b.$$

Ersetzt man hier x durch $-x$, so folgt

$$(f(-x))^2 = (f(x))^2,$$

und da $f(x)$ ein Polynom ungeraden Grades ist, folgt $f(-x) = -f(x)$ [2]). Es muß also $a_1 = a_3 = 0$ sein und daher

$$f(x) = a_0 x^3 + a_2 x. \tag{31$_1$}$$

Die Vertauschbarkeitsrelation lautet somit

$$(a_0 x^3 + a_2 x)^2 + b = a_0(x^2+b)^3 + a_2(x^2+b). \tag{32}$$

Hier treten rechts und links nur gerade Potenzen von x auf. Der Vergleich der Koeffizienten von x^6 in (32) ergibt

$$a_0 = 1. \tag{33}$$

Der Vergleich der Koeffizienten von x^4 liefert

$$a_2 = \tfrac{3}{2} b. \tag{34}$$

Vergleicht man nun noch die Koeffizienten von x^2 und x^0 in (32) und trägt in die so entstehenden beiden Gleichungen die Werte für a_0 und a_1 aus (33)

und (34) ein, so erhält man nach kurzer Rechnung die beiden Gleichungen für b

$$\begin{cases} b(b+2) = 0 \\ b(b+2)(2b-1) = 0, \end{cases} \tag{35}$$

denen b zu genügen hat, wenn

$$f(x) = x^3 + \tfrac{3}{2} b x$$

mit

$$g(x) = x^2 + b$$

vertauschbar sein soll. Die einzigen Werte b, die beide Gln. (35) erfüllen, sind

$$b = 0, \quad b = -2. \tag{36}$$

Hiernach gibt es höchstens zwei Grundketten, die eine mit dem quadratischen Polynom x^2 und die andere mit dem Polynom zweiten Grades $x^2 - 2$. Die Grundkette mit x^2 als quadratischem Polynom ist gerade die Kette (I). Die Frage ist, ob es eine Grundkette gibt, die

$$f_2(x) = x^2 - 2 \tag{30_1}$$

als Polynom zweiten Grades besitzt. Da nach (31_1), (33) und (34)

$$f_3(x) = x^3 - 3x \tag{31_2}$$

mit $f_2(x)$ vertauschbar ist, müßte die Grundkette so anfangen

$$f_1(x) = x, \quad f_2(x) = x^2 - 2, \quad f_3(x) = x^3 - 3x, \ldots.$$

Da ja das einzige Polynom vierten Grades, das mit f_2 vertauschbar ist (Satz 20), $f_2^2 = f_4(x) = x^4 - 4x^2 + 2$ ist, hätten wir von der vermuteten Kette schon 4 Glieder. Nun haben diese vier ersten Glieder alle den Eigenwert 2 gemeinsam. Daher ist zu vermuten, daß in der erwarteten Kette $f_0 = 2$ Eigenwert aller Kettenglieder sein wird. Wenn wir daher die Kette zu einer erweiterten Kette machen, beginnt sie:

$$f_0 = 2, \quad f_1 = x, \quad f_2 = x^2 - 2, \quad f_3 = x^3 - 3x, \quad f_4 = x^4 - 4x^2 + 2, \ldots.$$

Bei näherer Betrachtung dieser Polynome sieht man, daß sie die Rekursion

$$f_n = x \cdot f_{n-1} - f_{n-2}, \qquad n = 2, 3, 4 \tag{37}$$

erfüllen. Diese Rekursionsformel definiert sukzessive

$$f^5(x) = x^5 - 5x^3 + 5x, \quad f_6(x) = x^6 - 6x^4 + 9x^2 - 2, \ldots.$$

Wenn diese Polynome Glieder einer Kette sein sollen, muß z.B. $f_6(x) = f_2 f_3 = f_3 f_2$ sein, was man durch Rechnung bestätigt. Wenn wirklich die durch (37) rekursiv definierten $f_n(x)$ eine Kette darstellen, so zeigt (37) auch, daß alle Polynome der Kette den gemeinsamen Eigenwert 2 besitzen.

Definiert man noch

$$f_{-1} = x, \tag{37_1}$$

so gilt (37) schon von $n = 1$ an.

Nach Satz 23 brauchen wir zum Nachweise, daß die durch (37) definierten Polynome eine V-Kette bilden, nur zu zeigen, daß jedes $f_n(x)$ mit $f_2(x)$ vertauschbar ist. Es ist also

$$f_n(x^2 - 2) = (f_n(x))^2 - 2 \tag{38}$$

für alle n zu zeigen. Für $n = -1, 0, 2, 3, 4$ ist ja (38) richtig. Die Richtigkeit von (38) wird durch Induktion bewiesen. Dazu bemerken wir, daß der Ausdruck

$$(f_{n-1}(x))^2 + (f_n(x))^2 - x f_n(x) \cdot f_{n-1}(x)$$

vom Index n unabhängig ist. Denn ersetzt man in ihm nach (37) $f_n(x)$ durch $x f_{n-1} - f_{n-2}$, so geht er in den Ausdruck

$$(f_{n-2}(x))^2 + (f_{n-1}(x))^2 - x f_{n-1}(x) \cdot f_{n-2}(x)$$

über. Da der Ausdruck für $n = 1$ gleich $4 - x^2$ ist, gilt also

$$(f_{n-1})^2 + (f_n)^2 - x \cdot (f_n) \cdot (f_{n-1}) = 4 - x^2. \tag{37_2}$$

Nehmen wir nun an, daß (38) schon richtig ist für $r = 0, 1, 2, \ldots, n$:

$$f_r(x^2 - 2) = (f_r(x))^2 - 2, \tag{38_1}$$

so zeigen wir mit Hilfe von (37_2), daß (38_1) auch für $r = n + 1$ gilt. Dazu ersetzen wir in (37) x durch $x^2 - 2$ und erhalten

$$f_{n+1}(x^2 - 2) = (x^2 - 2) f_n(x^2 - 2) - f_{n-1}(x^2 - 2),$$

wenn wir (37) für den Index $(n + 1)$ benutzen. Wendet man rechts die schon für $r \leqq n$ als richtig angenommene Gl. (38_1) an, so erhält man nach kurzer Rechnung:

$$f_{n+1}(x^2 - 2) = (x \cdot f_n)^2 - 2\{x^2 + (f_{n-1})^2 + (f_n)^2\} + (f_{n-1})^2 + 6.$$

Da die geschweifte Klammer auf der rechten Seite nach (37_2) gleich

$$4 + x \cdot f_{n-1} \cdot f_n$$

ist, folgt unter nochmaliger Verwendung von (37)

$$f_{n+1}(x^2 - 2) = (f_{n+1}(x))^2 - 2,$$

womit die Richtigkeit von (38_1) auch für $r = n + 1$ gezeigt ist. Also gilt (38) stets und damit gibt (37) wirklich eine Grundkette

$$\text{(II)} \qquad \begin{cases} f_1 = x, \quad f_2 = x^2 - 2, \quad f_3 = x^3 - 3x, \ldots \\ f_{n+1} = x f_n - f_{n-1} \quad (n = 0, 1, 2, \ldots), \quad f_0 = 2, \quad f_{-1} = x. \end{cases}$$

Alle Polynome in (II) haben den Eigenwert 2. Jede V-Kette ist also entweder zu (I) oder zu (II) ähnlich. (I) und (II) sind in den beiden Klassen die Grundketten.

Wie in jeder Kette, so ist auch hier

$$f_m f_n = f_n f_m = f_{mn}. \tag{39}$$

Die Polynome der Kette (II) sind aus der Algebra wohlbekannt, und von dorther ergibt sich auch unmittelbar die Gl. (39). Setzt man nämlich für variables z

$$z + \frac{1}{z} = x, \quad s_n = z^n + z^{-n}, \quad n = 0, \pm 1, \pm 2, \ldots, \tag{40}$$

so ist $s_1 = x$ und

$$s_n s_1 = s_n x = s_{n+1} + s_{n-1},$$

$$s_{n+1} = x s_n - s_{n-1}, \quad s_0 = 2, \quad s_{-1} = s_1 = x.$$

Daher wegen (37)

$$s_n = f_n(x) = f_n\left(z + \frac{1}{z}\right) = z^n + z^{-n}. \tag{41}$$

Ersetzt man hier z durch z^m, so folgt sofort

$$\begin{aligned} z^{nm} + z^{-nm} = s_{mn} = f_{mn}(x) &= f_n(z^m + z^{-m}) \\ &= f_n f_m(x) \\ &= f_m f_n(x), \end{aligned}$$

womit alles von neuem gezeigt ist.

Nun steht schon bei J. F. RITT[1]) als Beispiel für vertauschbare Polynome das Beispiel der Tschebyscheffschen Polynome, wobei RITT die Vertauschbarkeit aus der Definitionsgleichung

$$\cos(n\varphi) = T_n(\cos\varphi), \quad n = 0, 1, 2, \ldots \tag{42}$$

erhält, indem er φ durch $m\varphi$ ersetzt. Diese Ritt-Tschebyscheffsche V-Kette ist also

$$T_1 = x, \quad T_2 = 2x^2 - 1, \ldots. \tag{III}$$

Diese Kette ist zu (II) ähnlich und geht aus (II) durch die Ähnlichkeitstransformation $T(2, 0)$ hervor, so daß

$$\frac{1}{2} f_n(2x) = T_n(x), \quad f_n(x) = 2\, T_n\left(\frac{x}{2}\right) \tag{43}$$

ist. Man erhält dies ja auch unmittelbar, indem man oben $z = e^{i\varphi}$, $x = 2\cos\varphi$

$$s_n = f_n(x) = f_n(2\cos\varphi) = 2\cos(n\varphi)$$

einführt. Aus (37) ergibt sich dann die Rekursionsformel für die Tschebyscheffschen Polynome.

Für die Polynome $f_n(x)$ hat man die explizite Darstellung[3])

$$f_n(x) = \sum_{k=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \left\{ 2\binom{n-k}{k} - \binom{n-k-1}{k} \right\} (-1)^k x^{n-2k}, \quad n = 1, 2, 3, \ldots. \tag{37$_3$}$$

[3]) Siehe JACOBSTHAL, E.: Über die Klasseninvariante linearer Abbildungen. II. Det Kongelige Norske Videnskab. Selsk. Forh. **26**, 10—15, (1953) [Gl. (15a) auf S. 12].

Es sei bemerkt, daß aus der Gleichung

$$\cos^2(n\varphi) = \psi_n(\cos^2\varphi)$$

Polynome definiert werden, die ebenfalls eine Kette der Klasse (II) bilden. Die Kette der $\psi_n(x)$ geht durch $T(\frac{1}{2}, \frac{1}{2})$ in die Ritt-Tschebyscheffsche Kette über. — Es soll noch auf eine bemerkenswerte Tatsache hingewiesen werden: Ist ein quadratisches Polynom mit einem kubischen Polynom vertauschbar, dann besitzen sie beide vertauschbare Polynome jeden Grades. Diese Tatsache wird durch Satz 35 wesentlich verschärft werden.

§ 8. Ein zahlentheoretischer Satz über vertauschbare Polynome.

Ist $g(x)$ ein Polynom eines Grades $\geqq 2$ mit algebraischen Zahlkoeffizienten, und ist $f(x)$ mit $g(x)$ vertauschbar, dann folgt aus § 6 leicht, daß die Koeffizienten von $f(x)$ auch algebraische Zahlen sind. Nun betrachten wir speziell solche Polynome $g(x)$, bei denen alle Koeffizienten *ganze* algebraische Zahlen sind, deren höchster sogar eine *Einheit* sein soll. Solche Polynome $g(x)$ wollen wir kurz G-Polynome nennen. Ihre Nullstellen sind bekanntlich ganze algebraische Zahlen. Ist der Grad eines G-Polynoms $g(x)$ größer als 1, so sind daher die Eigenwerte ganze Zahlen. Die Iterierten eines G-Polynoms sind ebenfalls G-Polynome. Wir haben später Verwendung für einen Satz über G-Polynome, der folgendermaßen lautet:

Satz 25. *Ist $g(x)$ ein G-Polynom eines Grades >1, so ist jedes mit $g(x)$ vertauschbare Polynom $f(x)$ positiven Grades ebenfalls ein G-Polynom.*

Beweis. Es sei

$$g(x) = b_0 x^n + b_1 x^{n-1} + \cdots + b_n, \qquad n \geqq 2,$$

worin alle b_k ganze algebraische Zahlen sind und b_0 eine Einheit ist. Ferner sei

$$f(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_m, \qquad m \geqq 1,$$

mit $g(x)$ vertauschbar. Nach (28_1) in § 6 ist dann

$$a_0^{n-1} = b_0^{m-1},$$

also a_0 auch eine Einheit. Der Fall, daß $f(x) = x$ ist, kann außer Betracht bleiben, da ja dann $f(x)$ ein G-Polynom ist. Der Fall $f(x) = x + b$, $b \neq 0$, ist nach Satz 9 unmöglich, da der Grad n von $g(x)$ größer als 1 ist. Die einzigen linearen Polynome $f(x)$, die in Frage kommen können, sind

$$f(x) = a_0 x + a_1,$$

worin a_0 eine von 1 verschiedene Einheit ist. In diesem Falle besitzt $f(x)$ einen einzigen Eigenwert. Jedes mit $g(x)$ vertauschbare Polynom $f(x) \not\equiv x$ hat also m Eigenwerte, worin m der Grad von $f(x)$ ist.

Sei ζ ein beliebiger Eigenwert von $f(x)$. Da $g(x)$ mit $f(x)$ vertauschbar ist, ist auch jede Iterierte g^p von g mit $f(x)$ vertauschbar; also ist nach Satz 11 jede der Zahlen $g^p(\zeta)$ auch ein Eigenwert von $f(x)$; deswegen enthält die Folge

$$g^0(\zeta) = \zeta, \quad g(\zeta), \quad g^2(\zeta), \ldots$$

nur endlich viele verschiedene Zahlen, da ja $f(x)$ nur m Eigenwerte hat. Es ist also für passende r, s, $r \geqq 0$, $s \geqq 1$

$$g^r(\zeta) = g^{r+s}(\zeta),$$

und dies ist eine algebraische Gleichung für ζ, deren Koeffizienten ganze algebraische Zahlen sind, deren höchster eine Einheit ist, da ja die Iterierte eines G-Polynomes wieder ein G-Polynom ist. Also ist ζ eine ganze algebraische Zahl. Alle Eigenwerte von $f(x)$ sind also ganze algebraische Zahlen. Ist nun $m = 1$, $f(x) = a_0 x + a_1$, so ist

$$\zeta = \frac{a_1}{1 - a_0}$$

eine ganze algebraische Zahl, also $a_1 = \zeta(1 - a_0)$ auch eine solche und $f(x)$ ein G-Polynom. Ist aber $m > 1$, und sind die m Eigenwerte von $f(x)$ etwa $\zeta_1, \zeta_2, \ldots, \zeta_m$, dann ist wegen $m > 1$ der höchste Koeffizient in $f(x) - x$ auch a_0 und daher

$$f(x) - x = a_0(x - \zeta_1) \ldots (x - \zeta_m),$$

$$f(x) = a_0(x - \zeta_1) \ldots (x - \zeta_m) + x,$$

worin a_0 eine Einheit und alle ζ_k ganze algebraische Zahlen sind. Also ist $f(x)$ ein G-Polynom, w. z. b. w.

§ 9. Hilfsbetrachtungen über eine Zahlfolge.

Die Frage, wann bei gegebenem $g(x)$ die Gl. (1) als Lösungen $f(x)$ nur die Iterierten von $g(x)$ besitzt, oder ob es noch andere Lösungspolynome $f(x)$ gibt, soll später für das reine Polynom $g(x) = x^r + a$, $(r = 2, 3, \ldots)$ und für alle quadratischen Polynome entschieden werden. Für die Beantwortung dieser Frage ist es von Wichtigkeit zu wissen, ob die Zahl 0 eine reguläre oder singuläre Zahl des Polynoms $g(x) = x^r + a$ ist. Man hat also die Zahlfolge

$$V_{g(0)} = \{g^{(n)}(0)\}_{n=0,1,2,\ldots}$$

zu betrachten. Unter Weglassung der ersten Zahl sind das die Zahlen

$$a_n = g^{(n+1)}(0), \quad n = 0, 1, 2, \ldots. \tag{44}$$

Es ist also

$$\begin{cases} a_0 = g(0) = a, \\ a_1 = g(a) = a^r + a, \\ a_2 = g(a_1) = a_1^r + a = (a^r + a)^r + a, \\ \vdots \end{cases} \tag{44$_1$}$$

$$a_{n+1} = a_n^r + a, \quad a_0 = a, \quad n = 0, 1, 2, \ldots. \tag{44$_2$}$$

Die a_n sind ganzzahlige Polynome von a,

$$\left\{\begin{array}{l} a_n = \psi_n(a), \\ \psi_{n+1}(a) = (\psi_n(a))^r + a, \quad \psi_0(a) = a. \end{array}\right. \tag{45}$$

Das niederste Glied in jedem dieser Polynome ist a, der höchste Koeffizient ist gleich 1. Die Gleichung $\psi_n(a) = 0$ hat also außer $a = 0$ nur Einheiten als Lösung, falls $n \geqq 1$ ist. Bei $n \geqq 1$ sind alle Glieder außer dem letzten durch a^r teilbar. Die Frage, ob 0 eine reguläre oder singuläre Zahl des Polynoms $g(x) = x_r + a$ ist, ist gleichbedeutend mit der Frage: Für welche a sind alle a_n verschieden und für welche a ist die Folge $\{a_n\}$ periodisch? Das letztere tritt dann und nur dann ein, wenn für zwei verschiedene Indizes l, m, $l < m$,

$$a_m = a_l, \tag{46}$$

$$\psi_m(a) = \psi_l(a) \tag{46$_1$}$$

ist. Ist dann m der kleinste Index, für den ein a_m gleich einem a_l mit $l < m$ wird, so sind die Zahlen $a_0, a_1, \ldots, a_{m-1}$ alle verschieden. Die ganze Folge enthält nur m verschiedene Zahlen; von a_l an wiederholen sich die Zahlen der Folge periodisch. Wenn $l \geqq 1$ ist, bilden die Zahlen $a_0, a_1, \ldots, a_{l-1}$ eine Vorperiode, deren Glieder untereinander und von allen folgenden Zahlen verschieden sind. Für $l = 0$ fehlt die Vorperiode und die Folge ist reinperiodisch. Da die Gln. (46), (46$_1$) algebraische Gleichungen mit ganzen Koeffizienten sind, deren höchster gleich 1 ist, wird die Folge (44) periodisch, wenn a eine ganze algebraische Zahl ist, die (46), (46$_1$) genügt. Diese Zahlen wollen wir *kritische* Zahlen für den Exponenten r nennen; die anderen Zahlen a sollen *gewöhnliche* Zahlen für den Exponenten r heißen. Für eine gewöhnliche Zahl a ist also 0 eine reguläre Zahl des Polynoms $x^r + a$, dagegen ist 0 eine singuläre Zahl des Polynoms, falls a eine kritische Zahl für den Exponenten r ist. Alle Lösungen der Gln. (46), (46$_1$) stellen die Gesamtheit der kritischen Zahlen dar. Unter ihnen befindet sich trivialerweise die Zahl 0, da $\psi_n(0) = 0$ für $n = 0, 1, 2, \ldots$ ist. Diese können wir später außer Betracht lassen. Für den Exponenten $r = 2$ sind z.B. einige kritische Zahlen a und die zugehörigen $\{a_n\}$ in der Tabelle angegeben:

$a_0 = a$	a_1	a_2	a_3	a_4	a_5 ...
0	0	0	0	0	0 ...
-1	0	-1	0	-1	0 ...
-2	2	2	2	2	2 ...
i	$-1+i$	$-i$	$-1+i$	$-i$	$-1+i$ ...
$-i$	$-1-i$	i	$-1-i$	i	$-1-i$ ...
⋮	⋮	⋮	⋮	⋮	⋮

Wir beweisen nun über die reellen kritischen Zahlen

Satz 26. *Für ungerades $r>2$ ist die einzige reelle kritische Zahl $a=0$. Für gerades $r\geqq 2$ sind $a=0$, $a=-1$ und $a=-\sqrt[r-1]{2}$ kritische Zahlen. Alle sonst noch etwa vorhandenen reellen kritischen Zahlen liegen zwischen $-\sqrt[r-1]{2}$ und -1.*

Beweis. Für $a>0$ ist ja

$$a_0<a_1<a_2<\cdots.$$

Also ist jede positive Zahl eine gewöhnliche Zahl. Da für ungerades r

$$\psi_n(-a)=-\psi_n(a)$$

ist, so folgt für ungerade r, daß auch jede negative Zahl a eine gewöhnliche Zahl ist. Daher ist $a=0$ die einzige reelle kritische Zahl für den ungeraden Exponenten r.

Sei nun $r=2, 4, 6, \ldots$ und $a<0$.

Für $a=-1$ sieht dann die Folge so aus wie in der Tabelle des Falles $r=2$, so daß -1 kritische Zahl ist. Für $a_0=a=-\sqrt[r-1]{2}$ wird $a_1=a_2=a_3=\cdots=-a_0=\sqrt[r-1]{2}$, so daß $-\sqrt[r-1]{2}$ kritische Zahl ist. (Siehe Tabelle für $r=2$.)

Für $a<-\sqrt[r-1]{2}$ ist $-a>\sqrt[r-1]{2}$ und daraus folgt der Reihe nach

$$-a^{r-1}>2,\quad -a^r<2a,\quad a_1=a^r+a>-a>0,\quad a_1>|a|,\quad a_1^r>a_0^r=a^r,$$

$a_2>a_1$ und daher

$$0<a_1<a_2<a_3<\cdots.$$

Also ist jedes $a<-\sqrt[r-1]{2}$ eine gewöhnliche Zahl. Ist nun schließlich $-1<a<0$, so zeigt man auf ähnlichem Wege wie eben, daß

$$-1<a_0<a_2<a_4<\cdots<a_5<a_3<a_1<0$$

ist, also sind alle a_n voneinander verschieden und a keine kritische Zahl. Wenn es also außer den drei genannten reellen kritischen Zahlen noch andere solche geben sollte, liegen sie zwischen $-\sqrt[r-1]{2}$ und -1, w. z. b. w.

Wir beweisen nun weiter

Satz 27. *Ist die kritische Zahl $a\neq 0$ so beschaffen, daß die zugehörige periodische Folge $\{a_n\}$ keine Vorperiode hat, also reinperiodisch ist, dann ist a eine algebraische Einheit. Ist dagegen eine Vorperiode vorhanden und existiert eine Primzahl q, die in einer Potenz a^λ, $1\leqq\lambda\leqq r-1$, aufgeht, dann ist notwendigerweise $r=q=2$ und a ist eine zu 2 assoziierte algebraische Zahl.*

Beweis. Die kritischen Zahlen sind ganze algebraische Zahlen. Sei $a\neq 0$ eine solche und m, l, $m>l$, die Minimalindizes, für welche die a definierenden Gln. (46), (46_1) gelten. Ist dann $\{a_n\}$ reinperiodisch, so ist $l=0$, $a_m=a_{m-1}^r+a=a_0=a$; also ist $a_{m-1}=0$ und wegen $a_0=a\neq 0$ ist $m-1>0$; $m\geqq 2$. Hieraus folgt:

$$a_{m-1}=0=a_{m-2}^r+a.$$

Das ist nach Division mit a eine algebraische Gleichung mit ganzen Koeffizienten, deren höchster und niederster gleich 1 ist. Also ist a eine Einheit.

Damit ist der erste Teil erledigt. — Nun sei a eine solche kritische Zahl $\neq 0$, daß $\{a_n\}$ eine Vorperiode hat. Es ist $l \geqq 1$. Aus (46) folgt dann

$$a_{m-1}^r = a_{l-1}^r,$$

$$a_{m-1} = \varepsilon a_{l-1},$$

worin ε eine r-te Einheitswurzel ist, die wegen der Minimaleigenschaft von m von 1 verschieden ist. Es sei ε eine primitive s-te Einheitswurzel, $s \geqq 2$, $r \equiv 0 \bmod s$. Da jedes a_n als tiefstes Glied das Glied a hat und alle vor ihm stehenden Glieder Exponenten $\geqq r$ besitzen, ergibt die Gleichung $a_{m-1} - \varepsilon a_{l-1} = 0$ nach Division mit a, daß

(a) $$1 - \varepsilon \equiv 0 \bmod a^{r-1}$$

ist. Falls es nun eine Primzahl q gibt, die in einer Potenz a^λ aufgeht, worin $1 \leqq \lambda \leqq r-1$ ist, so sei

(b) $$\left[\frac{r-1}{\lambda}\right] = \mu, \quad 1 \leqq \lambda\mu \leqq r-1.$$

Dann ist

(a_1) $$1 - \varepsilon \equiv 0 \,(q^{\lambda\mu}).$$

In dieser Kongruenz kann ε durch jede der $\varphi(s)$ konjugierten ε^t, $1 \leqq t \leqq s-1$, $(t, s) = 1$, ersetzt werden. Die Multiplikation der $\varphi(s)$ Kongruenzen (a_1) ergibt dann

(c) $$F_s(1) \equiv 0 \bmod q^{\lambda\mu\varphi(s)},$$

worin $F_s(x)$ das s-te Kreisteilungspolynom ist. Da nun $F_s(1) = 1$ ist, falls s durch zwei verschiedene Primzahlen teilbar ist, und $F_s(1) = p$ ist, falls s die Potenz einer Primzahl p ist, folgt, daß wegen (c)

$$s = q^\alpha$$

sein muß und

$$q \equiv 0 \bmod q^{\lambda\mu\varphi(s)}.$$

Also folgt

$$\lambda\mu\varphi(s) = 1, \quad \lambda = 1, \quad \mu = 1, \quad \varphi(s) = 1, \quad s = 2 = q^\alpha, \quad q = 2, \quad \alpha = 1.$$

Wegen (b) ist $r - 1 = 1$, $r = 2$. Da $s = 2$ ist, wird $\varepsilon = -1$ und daher nach (a) die ganze algebraische Zahl a ein Teiler von $1 - \varepsilon = 2$. Es war aber $q = 2$ nach Annahme ein Teiler von $a^\lambda = a^1 = a$. Also ist 2 zu a assoziiert und der Satz bewiesen. Für den Exponenten $r = 2$ ist ja die kritische Zahl -2 zu 2 assoziiert. Wir beweisen nun

Satz 28. *Für den Exponenten $r = 2$ ist -2 die einzige zu 2 assoziierte kritische Zahl.*

Beweis. Die a_n sind bei $r = 2$ durch

$$a_{n+1} = a_n^2 + a, \quad a_0 = a,$$

definiert:

$$a_0 = a, \quad a_1 = a^2 + a, \quad a_2 = (a^2 + a)^2 + a, \ldots.$$

Rechnet man hier, um die kritischen Zahlen a zu erhalten, die niedersten Fälle der Gleichung $a_m = a_l$, $m > l$, durch, also die Fälle:

$$\begin{aligned} a_1 = a; \quad a_2 = a; \quad a_3 = a; \\ a_2 = a_1; \quad a_3 = a_1; \\ a_3 = a_2, \end{aligned}$$

so erhält man als kritische Zahlen:

$$0, \ -1, \ -2, \ +i, \ -i;$$

außerdem noch aus $a_3 = a$ die Lösungen von

$$a^3 + 2a^2 + a + 1 = 0,$$

die Einheiten sind, und im Falle $a_3 = a_2$ noch die Gleichung

$$a^3 + 2a^2 + 2a + 2 = 0.$$

Aus ihr folgt, daß $a \mid 2$; $a^2 \mid 2$; $a^3 \mid 2$ ist. Also ist

$$2 = a^3 \eta,$$

worin η eine ganze algebraische Zahl ist. Also bekommt man

$$\begin{aligned} a^3 + a^5 \eta + a^4 \eta + a^3 \eta = 0 \\ 1 + \eta (a^2 + a + 1) = 0. \end{aligned}$$

Daher ist η eine Einheit. Da a^3 keine Einheit ist, ist a^2 und $a^2 \eta$ keine Einheit, also auch $2/a$ keine Einheit, a also nicht zu 2 assoziiert.

In den niedersten Fällen ist also die einzige kritische zu 2 assoziierte Zahl -2.

Es ist daher für $N = 4$ richtig, daß unter allen kritischen Zahlen, die man aus

$$a_m = a_l, \quad l < m < N = 4$$

erhält, -2 die einzige zu 2 assoziierte Zahl ist. Wir nehmen nun an, es sei für eine positive ganze Zahl N richtig, daß unter allen kritischen Zahlen a, die sich aus allen Gleichungen

$$a_m = a_l, \quad 0 \leq l < m < N$$

ergeben, -2 die einzige zu 2 assoziierte Zahl ist. Wenn wir dann zeigen können, daß die N Gleichungen $a_N = a_l$, $l = 0, 1, \ldots, N-1$ außer -2 keine zu 2 assoziierte Zahl liefern, dann ist die Richtigkeit der Annahme auf alle Gleichungen

$$a_m = a_l, \quad 0 \leq l < m < N + 1$$

ausgedehnt, und da der Satz für $N = 2, 3, 4$ richtig war, gilt er dann allgemein.

Von den N Gleichungen $a_N = a_l$ ist die erste $a_N = a$, die $a_{N-1} = 0$ ergibt. Das ergibt außer $a = 0$ nur Einheiten a, also keine zu 2 assoziierte Zahl. Sei also $1 \leq l \leq N-1$. Dann ergibt die Gleichung $a_N = a_l$, daß $a_{N-1}^2 = a_{l-1}^2$ ist. Also wird $a_{N-1} = a_{l-1}$ oder $a_{N-1} = -a_{l-1}$. Von der ersten dieser Gleichungen stammen nach Annahme nur kritische Zahlen, die nicht zu 2 assoziiert sind, außer etwa -2. Also brauchen wir nur noch die zweite Gleichung

$$a_{N-1} + a_{l-1} = 0$$

zu betrachten. Für $l=1$ ergibt sich die Gleichung

$$a_{N-1}+a_0=a_{N-1}+a=0$$

oder

$$\psi_{N-1}(a)+a=0.$$

Nun ist das Polynom $\psi_{N-1}(x)+x$ gleich 0 für $x=0$ und $x=-2$. Also ist $\psi_{N-1}(x)+x$ durch $x(x+2)$ teilbar. Da $N\geqq 4$, $N-1\geqq 3$ ist, sind x^2+x die beiden niedersten Glieder in $\psi_{N-1}(x)$, daher sind die beiden niedersten Glieder in $\psi_{N-1}(x)+x$ gerade $x^2+x+x=x(x+2)$. Wenn man also $\psi_{N-1}(x)+x$ durch $x(x+2)$ dividiert, erhält man ein Polynom mit ganzen Koeffizienten, von denen der höchste und tiefste gleich 1 ist. Also hat die Gleichung $\psi_{N-1}(a)+a=0$ als Lösungen nur $a=0$, $a=-2$ und außerdem nur Einheiten. Nun sei $l\geqq 2$. Da sind a^2 und a die niedersten Glieder in a_{N-1} und a_{l-1}. Daher endet $a_{N-1}+a_{l-1}$ mit den beiden Gliedern $2a^2+2a$. Nach Abspaltung des Faktors a endet also das übrigbleibende Polynom mit

$$\cdots+2a+2.$$

Die nach Abspaltung des Faktors a aus $a_{N-1}+a_{l-1}=0$ entstehende Gleichung

$$\cdots+2a+2=0$$

zeigt also, daß 2 durch die kritische Zahl a und daher sogar durch a^2 teilbar wird. Es ist also $2=a^2\eta$, worin η eine ganze algebraische Zahl ist. Da 2 keine Einheit ist, können nicht gleichzeitig a und η Einheiten sein, also ist auch $a\eta=2/a$ keine Einheit, also ist die kritische Zahl a nicht zu 2 assoziiert, womit durch Induktionsschluß der Satz bewiesen ist.

Aus Satz 27 und 28 folgt nun

Satz 29. *Ist $a\neq 0$ eine kritische Zahl für den Exponenten r und ist a durch eine Primzahl teilbar, dann ist $r=2$ und $a=-2$.*

Beweis. Ist nämlich a durch eine Primzahl q teilbar, dann ist a keine Einheit; die zu a gehörige Folge $\{a_n\}$ hat nach Satz 27 eine Vorperiode und nach demselben Satz ist $r=2$ und a zu 2 assoziiert. Nach Satz 28 aber ist bei $r=2$ die einzige zu 2 assoziierte kritische Zahl $a=-2$, womit alles gezeigt ist.

§ 10. Das Polynom $g(x)=x^r+a$.

Wir setzen voraus, daß der Grad $r\geqq 2$ und $a\neq 0$ ist, und beweisen

Satz 30. *Jedes mit $g(x)$ vertauschbare Polynom $f(x)$ des Grades $n>0$ hat die Gestalt*

$$f(x)=c_n x^n+c_{n-r}x^{n-r}+c_{n-2r}x^{n-2r}+\cdots \quad (47)$$

[4]) Dieser Satz gilt allgemein, wenn $g(x)$ nur Potenzen von x^r enthält. Dann ist für eine primitive r-te Einheitswurzel ε stets $g(\varepsilon x)=g(x)$, und wenn $fg=gf$ ist, folgt $gf(x)=fg(x)=fg(\varepsilon x)=gf(\varepsilon x)$. Aus $g(f(\varepsilon x))-g(f(x))=0$ läßt sich dann der Faktor $(f(\varepsilon x))^r-((fx))^r$ abspalten, und die Untersuchung des höchsten Gliedes des Restfaktors zeigt, daß er $\neq 0$ ist, so daß man (49) erhält, woraus nach dem Beweis im Text alles Weitere folgt.

Beweis. Da $fg = gf$ ist, gilt

$$f(x^r + a) = (f(x))^r + a. \tag{48}$$

Bedeutet ε eine primitive r-te Einheitswurzel, so bleibt die linke Seite von (48) unverändert, wenn man x durch εx ersetzt. Da also auch die rechte Seite sich nicht ändert, folgt

$$(f(\varepsilon x))^r = (f(x))^r. \tag{49}$$

Daher wird

$$f(\varepsilon x) = \varepsilon^c (f(x)), \tag{50}$$

worin c eine passende ganze Zahl ist. Ist nun

$$f(x) = \sum_{\nu=0}^{n} c_\nu x^\nu, \qquad c_n \neq 0, \tag{51}$$

so folgt aus (50) durch Koeffizientenvergleichung

$$c_\nu \varepsilon^\nu = \varepsilon^c c_\nu, \qquad \nu = 0, 1, \ldots, n. \tag{52}$$

Insbesondere für $\nu = n$ wegen $c_n \neq 0$

$$\varepsilon^n = \varepsilon^c.$$

Daher ist

$$c_\nu (\varepsilon^n - \varepsilon^\nu) = 0. \tag{52_1}$$

Hieraus folgt, daß alle Koeffizienten $c_\nu = 0$ werden, bei denen $n - \nu \not\equiv 0 \bmod r$ ist. Das Polynom $f(x)$ enthält also nur solche Glieder $c_\nu x^\nu$, bei denen $n - \nu = \lambda r$, $\nu = n - \lambda r$ ist, w. z. b. w.

Nun teilen wir alle mit $g(x^r) = x + a$ vertauschbaren Polynome positiven Grades in zwei Abteilungen ein:

Abteilung A enthält alle diejenigen $f(x)$, die einen durch r teilbaren Grad n haben. — Für jedes $f(x)$ in A ist der Grad $\geq r$.

Abteilung B enthält alle übrigen mit $g(x)$ vertauschbaren Polynome $f(x)$.

Zu A gehört $g(x)$ und alle Iterierten g^q, $q \geq 1$. Zu B gehört $f(x) \equiv x$. Es kann sein, daß B nur aus diesem Polynom besteht.

Satz 31. *In B ist $f(x) \equiv x$ das einzige Polynom, das einen Grad $n < r$ besitzt.*

Beweis. Ist nämlich für ein Polynom $f(x)$, das mit $g(x)$ vertauschbar ist, der Grad $n < r$, so ist wegen (47) $f(x)$ von der Gestalt

$$f(x) = c_n x^n.$$

Daher erhalten wir aus (48) die Beziehung

$$c_n (x^r + a)^n = c_n^r x^{nr} + a, \tag{53}$$

die nur für $n = 1$ möglich ist und dann $c_n = 1$, also $f(x) \equiv x$ ergibt.

Satz 32. *Jedes Polynom $f(x)$ der Abteilung A läßt sich zusammensetzen aus einer Iterierten g^q, $q \geq 1$, und einem Polynom $F(x)$ der Abteilung B.*

Beweis. $f(x)$ habe den Grad n, der durch r teilbar ist. Wir nehmen an, daß die höchste Potenz von r, die in n aufgeht, die q-te Potenz ist, und setzen

$$n = r^q n'; \quad n' \not\equiv 0 \bmod r. \tag{54}$$

Wir bezeichnen $f(x)$ mit $f_0(x)$, dann treten in $f_0(x)$ wegen (47) nur solche Glieder auf, deren Exponenten Multipla von r sind; also ist

$$f_0(\sqrt[r]{x-a}) = f(\sqrt[r]{x-a}) = f_1(x) \tag{55}$$

ein Polynom von x mit dem höchsten Koeffizienten c_n und dem Grade

$$n_1 = \frac{n}{r} = r^{q-1} n'; \quad n = n_0; \quad n_1 = \frac{n_0}{r}. \tag{56}$$

Dieses neue Polynom $f_1(x)$ ist ebenfalls mit $g(x)$ vertauschbar, denn es ist

$$f_1 g = f(\sqrt[r]{g(x)-a}) = f(x) = f_0(x),$$

da $g(x) - a = x^r$ ist. Und es wird

$$\begin{aligned} g f_1 &= g f(\sqrt[r]{x-a}) = f g(\sqrt[r]{x-a}) \\ &= f(x-a+a) = f(x) = f_0(x). \end{aligned}$$

$$f_1 g = g f_1 = f_0 = f. \tag{57}$$

Ist nun $q = 1$, so ist $n_1 = n'$, also der Grad von f_1 nicht durch r teilbar. Ist aber $q > 1$, so ist der Grad von f_1 noch durch r teilbar und f_1 hat, da es mit g vertauschbar ist, nur solche Glieder, deren Exponenten Multipla von r sind. Dann wird nach demselben Schlußverfahren

$$f_1(\sqrt[r]{x-a}) = f_2(x) \tag{55$_1$}$$

ein mit g vertauschbares Polynom des Grades

$$n_2 = \frac{n_1}{r} = r^{q-2} n, \tag{56$_1$}$$

und analog zu (57)

$$f_2 g = g f_2 = f_1. \tag{57$_1$}$$

Bei $q = 2$ sind wir am Ende des Verfahrens, bei $q > 2$ setzen wir es fort, bis zum ersten Male in der Reihe der abnehmenden Grade $n = n_0, n_1, n_2, \ldots$ ein durch r unteilbarer Grad $(= n')$ auftaucht. Wir erhalten also der Reihe nach die Polynome $f_0, f_1, f_2, \ldots, f_q$ mit den Gradzahlen

$$n_0, n_1, n_2, \ldots, n_q = n'$$

durch die Formeln

$$f_\lambda(\sqrt[r]{x-a}) = f_{\lambda+1}(x), \quad \lambda = 0, 1, \ldots, q-1. \tag{55'}$$

Der Grad von $f_\lambda(x)$ ist

$$n_\lambda = \frac{n_0}{r^\lambda} = r^{q-\lambda} n', \quad \lambda = 0, 1, 2, \ldots, q. \tag{56'}$$

$$f_\lambda g = g f_\lambda = f_{\lambda-1}, \quad \lambda = 1, 2, \ldots, q. \tag{57'}$$

Alle f_λ haben denselben höchsten Koeffizienten c_n und

$$F(x) = f_q(x) \tag{58}$$

hat den durch r unteilbaren Grad $n_q = n'$. Aus (57') erhält man durch sukzessive Anwendung ($\lambda = 1, 2, \ldots, q$):

$$f_0 = f = g f_1 = g^2 f_2 = g^3 f_3 = \cdots = g^q f_q = g^q F = F g^q$$

$$f(x) = F g^q = g^q F. \tag{59}$$

Da der Aufbau der Polynome $f(x)$ in A nach Satz 31 auf Polynome $F(x)$ in B führt, betrachten wir nun nur noch Polynome $f(x)$ der Abteilung B. Enthält die Abteilung B außer $f(x) = x$ noch andere Polynome, so sei $f(x)$ eines von diesen, also nach Satz 30: $n \geqq r$, $n \not\equiv 0 \bmod r$.

Satz 33. *Hat das Polynom $f(x)$ der Abteilung B einen Grad $n > r$, so ist notwendigerweise $r = 2$ und $a = -2$, d.h. wenn $g(x) \equiv x^2 - 2$ ist, besteht die Abteilung B nur aus dem Polynom $f(x) = x$.*

Beweis. Da $n \not\equiv 0 \bmod r$ ist, folgt aus (47), daß $f(x)$ kein konstantes Glied besitzt; also ist $f(0) = 0$ und somit 0 ein Eigenwert des Polynoms $f(x)$. Nun ist jede Iterierte von $g(x)$ mit $f(x)$ vertauschbar. Und deswegen ist nach Satz 11 jede der Zahlen $g^m(0)$ ein Eigenwert von $f(x)$; da aber $f(x)$ nur n Eigenwerte hat, enthält die Folge der Zahlen $a_m = g^{m+1}(0)$ nur endlich viele verschiedene, und somit ist a eine kritische Zahl für den Exponenten r. Da eine solche aber eine ganze algebraische Zahl ist, ist $g(x) = x^r + a$ ein G-Polynom und deswegen nach Satz 25 auch $f(x)$ ein solches. Daher sind die Koeffizienten $c_n, c_{n-r}, c_{n-2r}, \ldots$ in (47) ganze algebraische Zahlen, c_n eine Einheit, die nach (28_1) eine $(r-1)$-te Einheitswurzel sein muß, was sich ja aus $fg = gf$ oder

$$c_n (x^r + a)^n + c_{n-r}(x^r + a)^{n-r} + \cdots = (c_n x^n + c_{n-r} x^{n-r} + \cdots)^r + a$$

durch Koeffizientenvergleich der höchsten Glieder ergibt. Das zweithöchste Glied hat den Exponenten $r(n-1)$. Der Koeffizient von $x^{r(n-1)}$ auf der linken Seite ist $n c_n a$ und auf der rechten Seite $r c_n^{r-1} c_{n-r} = r c_{n-r}$. Daher erhalten wir

$$c_{n-r} = \frac{n a}{r} c_n. \tag{60}$$

Hierin ist c_n eine Einheit, c_{n-r} eine ganze algebraische Zahl, also $\frac{n a}{r}$ eine ganze algebraische Zahl; nun ist $\frac{n}{r}$ keine ganze Zahl, daher enthält r einen Primfaktor q, der in der kritischen Zahl a aufgeht. Also ist nach Satz 29 $a = -2$, $r = 2$, womit Satz 32 bewiesen ist.

Durch Satz 31 und Satz 32 erhalten wir zusammenfassend

Satz 34. *Für das Polynom $g(x) = x^r + a$, $r \geqq 2$, $a \neq 0$ ist die Folge V_g der Iterierten von g im allgemeinen vollständig, d.h. außer den Iterierten von g gibt es kein Polynom $f(x)$ positiven Grades, das mit $g(x)$ vertauschbar ist. Die einzige Ausnahme ist $g(x) = x^2 - 2$, das das quadratische Polynom der Grundkette* (II) *in § 7 ist. V_g ist nur eine Teilfolge der Kette* (II).

Der Fall $a=0$, $g(x)=x^r$, $r\geqq 2$ erledigt sich leicht. V_g ist nicht vollständig. Denn alle Lösungen von

$$fg=gf, \qquad f(x^r)=(f(x))^r$$

sind nach den Bemerkungen, die im Anschluß an Satz 19 gemacht wurden:

$$f(x)=C\,x^m, \quad C^{r-1}=1, \quad m=0,1,2,\ldots,$$

wozu noch $f(x)\equiv 0$ kommt.

§ 11. Quadratische Polynome.

Ist $g(x)$ ein beliebiges Polynom positiven Grades und V_g die zugehörige Folge (4) der Iterierten von g, und transformiert man durch eine Ähnlichkeitstransformation T, (§ 5), g in g_1, so geht bei Anwendung desselben T auf alle Elemente von V_g diese Folge in V_{g_1} über. Die Folgen heißen ähnlich. Ist die eine vollständig, so ist die andere auch vollständig. Nun sei

$$g(x)=a_0x^2+a_1x+a_2, \qquad a_0\neq 0, \tag{61}$$

ein gegebenes quadratisches Polynom. Bezeichnet man die Diskriminante von $g(x)$ mit D, also

$$D=a_1^2-4a_0a_2, \tag{61$_1$}$$

und setzt man

$$I(g)=I=D-2a_1=a_1^2-4a_0a_2-2a_1, \tag{61$_2$}$$

so ist I eine Invariante der Transformation. Geht also g durch die Transformation $T(c,d)$, § 5, Gl. (22), in

$$g_1(x)=b_0x^2+b_1x+b_2 \tag{62}$$

über und ist

$$\Delta=b_1^2-4b_0b_2, \tag{62$_1$}$$

$$I(g_1)=\Delta-2b_1=b_1^2-4b_0b_2-2b_1, \tag{62$_2$}$$

so ist

$$I(g)=I(g_1) \tag{63}$$

und umgekehrt folgt aus (63), daß (61) und (62) ähnliche Polynome sind, die durch die Transformation $T(c,d)$ mit

$$c=\frac{b_0}{a_0}, \qquad d=\frac{b_1-a_1}{2a_0} \tag{64}$$

ineinander transformiert werden, d.h. es ist

$$g_1=T^{-1}fT(x). \tag{65}$$

Nun gibt es nach § 5 eine einzige Transformation T, die $g(x)$ in $g_1(x)=x^2+a$ transformiert. Es ist also bei Anwendung dieser Transformation

$$b_0=1, \quad b_1=0, \quad b_2=a, \quad \Delta=-4a, \quad I(g_1)=-4a.$$

Also

$$a_1^2 - 4a_0a_2 - 2a_1 + 4a = 0. \tag{63_1}$$

Wegen Satz 34 und der anschließenden Bemerkungen ist V_{g_1} eine vollständige Folge dann und nur dann, wenn $a \neq 0$, $a \neq -2$; also ist V_g dann und nur dann vollständig, wenn

$$I(g) = a_1^2 - 4a_0a_2 - 2a_1 \neq 8 \quad \text{und} \quad \neq 0$$

ist. Ist dagegen $I(g) = 0$ oder 8, so liegt g in einer V-Kette, die zu (I) oder (II), s. § 7, ähnlich ist. Wir bekommen so

Satz 35. *Ist* $g(x) = a_0x^2 + a_1x + a_2$, $a_0 \neq 0$, *ein quadratisches Polynom, so sind im allgemeinen die einzigen Polynome positiven Grades, die mit* $g(x)$ *vertauschbar sind, die Iterierten von* $g(x)$. *Nur wenn* $I(g) = a_1^2 - 4a_0a_2 - 2a_1 = 0$ *oder* $= 8$ *ist, gibt es für jeden positiven Grad* m *genau ein Polynom* $f(x)$, *das mit* $g(x)$ *vertauschbar ist. Man bekommt es im Falle* $I(g) = 0$ *aus dem Gliede* x^m *der Kette* (I) *und im Falle* $I(g) = 8$ *aus dem Gliede* $f_m(x)$ *der Kette* (II) *durch eine Ähnlichkeitstransformation.*

Für die quadratischen Polynome $g(x)$ und die reinen Polynome ist in den beiden letzten Paragraphen die Frage nach der Vollständigkeit der Folge der Iterierten von $g(x)$ entschieden worden. Man kann sehr leicht Polynomklassen angeben, bei denen die zugehörige Folge V_g nicht vollständig ist. Ist nämlich ε eine r-te Einheitswurzel $\neq 1$ und

$$g(x) = \sum_{\lambda=0}^{q} a_{\lambda r+1} x^{\lambda r+1}$$

ein Polynom des Grades $m = qr + 1$, so ist

$$g(\varepsilon g(x)) = \varepsilon \sum_{\lambda=0}^{q} a_{\lambda r+1} (g(x))^{\lambda r+1} = \varepsilon g(g(x)).$$

Es ist also

$$f(x) = \varepsilon g(x)$$

mit $g(x)$ und daher mit jedem Element von V_g vertauschbar, ohne daß $f(x)$ ein Element von V_g ist. V_g ist also nicht vollständig.

Matematisk Institutt, Norges Tekniske Høgskole, Trondheim (Norwegen).

(Eingegangen am 18. März 1955.)

Keller, O.-H.
Math. Zeitschr. Bd. 63, S. 277—285 (1955)

Eine Bemerkung zur Ausführung der körpertheoretischen Operationen in erträglich vielen Schritten.

Dem Gedächtnis von Issai Schur.

Von

Ott-Heinrich Keller.

Wohl die eindrucksvollste Vorlesung, die ich als Student hörte, war die von I. Schur im Wintersemester 1926/27 über Galoissche Theorie. Es sei mir daher gestattet, meine Verehrung für ihn durch eine bescheidene Bemerkung zur Galoisschen Theorie zu bezeugen.

Wie allen Studenten war es auch mir eine große Enttäuschung, daß die Galoissche Theorie auch im Fall einer auflösbaren Gruppe die Berechnung der Wurzeln zwar theoretisch, aber nicht praktisch möglich macht. Und mir ist das Bild und der Tonfall des Augenblicks noch gegenwärtig, als Schur sagte, daß die Galoissche Resolvente einer Gleichung 5. Grades im allgemeinen vom 60. Grade sei. Es ist nicht der hohe Grad allein, der die Rechnung so sehr verwickelt. Sondern es werden, etwa beim Satz vom primitiven Element, Unbestimmte eingeführt, und man muß dann mit Polynomen in mehreren Veränderlichen rechnen. Es wird zwar gezeigt, daß es immer Zahlen gibt, durch die man diese Unbestimmten ersetzen darf, aber das sind reine Existenzaussagen und diese werden in keinem der üblichen Lehrbücher zu einem Konstruktionsverfahren ausgebaut. Hier einen noch so kleinen und unscheinbaren Schritt weitergehen zu können, scheint mir eine Mitteilung zu rechtfertigen. Der Grundgedanke findet sich in einer Arbeit von I. Schur[1]). Die angegebene Vereinfachung wird uns im IV. Abschnitt in den Stand setzen, die Galoissche Gruppe einer numerisch gegebenen Gleichung 5. Grades mit erträglichem Aufwand zu berechnen.

I.

Dieser kleine Schritt ist in dem folgenden Satz enthalten.

Satz. Es sei G ein Integritätsbereich, K sein Quotientenkörper. K sei separabel und enthalte unendlich viele Elemente. Die Zahlen α und β seien ganz algebraisch über G; β möge der irreduziblen Gleichung $f(\beta)=0$ über G genügen. *Es sei u eine Zahl aus G, die in der Diskriminante von f nicht aufgeht. Dann ist $\beta+u\alpha$ ein primitives Element des Körpers $K(\alpha,\beta)$.*

Um den Satz zu beweisen, denken wir uns die Konjugierten $\beta=\beta_1$, $\beta_2,\ldots,\beta_r$ und $\alpha=\alpha_1$, $\alpha_2,\ldots,\alpha_s$ von β und α hingeschrieben. Angenommen,

[1]) Schur, I.: Zur Irreduzibilität der Kreisteilungsgleichung. Math. Z. **29**, 463 (1928).

unter den Größen $\beta_i + u\alpha_k$ $(i = 1, \ldots, r;\ k = 1, \ldots, s)$ seien zwei gleiche, $\beta_{i_1} + u\alpha_{k_1} = \beta_{i_2} + u\alpha_{k_2}$, so wäre $\beta_{i_1} - \beta_{i_2} = u(\alpha_{k_2} - \alpha_{k_1})$, und u wäre ein Teiler von $\beta_{i_1} - \beta_{i_2}$ und damit auch von der Diskriminante von f. Also sind die $\beta_i + u\alpha_k$ alle verschieden. Daraus kann man in der üblichen Weise schließen, daß $\beta + u\alpha$ ein primitives Element des Körpers $K(\alpha, \beta)$ ist.

II.

Es sei nun ein Polynom $g(x; \alpha)$ mit Koeffizienten aus $G[\alpha]$ gegeben. Will man $g(x; \alpha)$ in irreduzible Faktoren zerlegen, so bildet man üblicherweise die Norm $F(x; u) = N\big(g(x - u\alpha; \alpha)\big)$ mit einer Unbestimmten u und zerlegt F in Faktoren $F = F_1 \cdot F_2 \ldots F_n$. Dann sind die Faktoren von g die größten gemeinsamen Teiler der F_i mit g[2]). Mit unbestimmten u ist diese Rechnung auch in einfachen Fällen nicht mehr in erträglich vielen Schritten zu bewältigen. Ist α etwa eine Irrationalität 5. Grades, so bedeutet die Normbildung die Berechnung einer Determinante 5. Grades, deren Elemente Polynome in x und u sind. Weiter hätten wir dann die Zerlegung eines Polynoms sehr hohen Grades in zwei Veränderlichen in Faktoren zu zerlegen. Für die Rechnung ist es daher sehr vorteilhaft zu wissen, *daß das u dabei durch irgendeine Zahl ersetzt werden darf, die nur nicht in der Diskriminante eines irreduziblen Teiles von* $N\big(g(x; \alpha)\big)$ *aufgeht.* Zum Beweise bezeichnen wir die Konjugierten von α mit $\alpha_1, \ldots, \alpha_s$, die Nullstellen von $g(x, \alpha_k)$ mit $\beta_i^{(k)}$ $(i = 1, \ldots, r;\ k = 1, \ldots, s)$. Dann ist $g(x, \alpha_k) = \prod_{i=1}^{r} (x - \beta_i^{(k)})$ und $N\big(g(x; \alpha_k)\big) = \prod_{i=1}^{r} \prod_{k=1}^{s} (x - \beta_i^{(k)})$, also die Gleichung für $\beta_i^{(k)}$ über K oder ein Vielfaches von ihr. Es ist $F(x; u) = \prod_{i=1}^{r} \prod_{k=1}^{s} (x - u\alpha_k - \beta_i^{(k)})$, zerfällt also nach dem bewiesenen Satz in die irreduziblen Polynome, deren Nullstellen die primitiven Elemente der Körper $K_{ik}(\alpha_k, \beta_i^{(k)})$ sind. Der größte gemeinsame Teiler eines solchen Teilpolynoms mit $g(x - u\alpha, \alpha)$ hat als Nullstellen genau eine solche Reihe von Größen $u\alpha + \beta_k^{(1)}$ $(k = k_1, k_2, \ldots)$ die über $K(\alpha)$ konjugiert sind, ist also irreduzibel.

Ist die Diskriminante von $N\big(g(x; \alpha)\big)$ nicht ohne weiteres berechenbar, so bilde man $N\left(u^r g\left(\frac{x - \alpha}{u}; \alpha\right)\right) = \prod_{k=1}^{s} \prod_{i=1}^{r} (x - \alpha_k - u\beta_i^{(k)})$, wo u jetzt in der Diskriminante der irreduziblen Gleichung $f(\alpha) = 0$ für α nicht aufgehen möge.

III.

Es sei jetzt eine irreduzible Gleichung $f(x) = 0$ vom n-ten Grade vorgelegt, die wir mit Hilfe der Galoisschen Theorie behandeln sollen; es sei α eine Wurzel. Wir können die Gleichung $g(x; \alpha) = \frac{f(x)}{x - \alpha}$ für die übrigen Wurzeln bestimmen. Es sei β eine Wurzel von g und damit auch von f. Eine Gleichung für ein primitives Element des Körpers $K(\alpha, \beta)$ ist dann ein Teiler von $F(x) = N\big(g(x - u\alpha; \alpha)\big)$, wo u nur in der Diskriminante von f nicht aufgehen möge.

[2]) WAERDEN, VAN DER: Moderne Algebra I, 1. Aufl., § 37, S. 128. 1930.

Diese Norm ist in den einfachsten nicht trivialen Fällen noch mit erträglichem Aufwand zu berechnen. Dieses F ist freilich noch nicht die Galoissche Resolvente, sondern erst eine Wiederholung des Verfahrens führt zu ihr hin. Es scheint aber zweckmäßig, erst einmal das F auszunutzen. Wir erhalten wesentliche Aufschlüsse über die Galoissche Gruppe, wenn wir F in irreduzible Faktoren zerlegen. Diese Faktorzerlegung mag mühevoll sein; sie ist aber nach einem Satz von KRONECKER[3]) prinzipiell möglich. Die dort angegebene Methode ist aber praktisch nicht ausführbar, und wir werden uns für unseren Fall andere Ansätze suchen müssen. Zunächst ist F im Restklassenkörper mod u zerlegbar in $(f(x))^{n-1}$, denn es ist $N(g(x;\alpha)) = (f(x))^{n-1}$. Die Teiler von F werden also als Grad ein Vielfaches von n haben. Suchen wir eine Zerlegung $F = P\,Q$ in Polynome bestimmter, durch n teilbarer Grade, so denken wir uns, wenn u eine Primzahl ist, P und Q u-adisch entwickelt: $P = \sum_i p_i u^i$, $Q = \sum_i q_i u^i$. Dann sind uns p_0 und q_0 als Potenzen von f bekannt. Wir können nun die Koeffizienten der verschiedenen Potenzen von u rechts und links miteinander vergleichen. Wir bilden zunächst $\frac{1}{u}(F - p_0 q_0) \equiv p_1 q_0 + q_1 p_0 \pmod{u}$ und können p_1 und q_1 aus dieser Kongruenz, wenn überhaupt, dann linear berechnen. Die Vieldeutigkeit in der Bestimmung von p_1 und q_1 können wir ausnutzen, um die nächste Kongruenz

$$\frac{1}{u}\left(\frac{1}{u}(F - p_0 q_0) - p_1 q_0 - p_0 q_1\right) - p_1 q_1 \equiv p_2 q_0 + q_2 p_0 \pmod{u}$$

lösbar zu machen, wenn dies überhaupt möglich ist. Diese Kongruenz ist doch dann und nur dann lösbar, wenn die linke Seite durch den größten gemeinsamen Teiler von p_0 und q_0 teilbar ist. So fortfahrend kommen wir entweder auf eine unlösbare Kongruenz oder auf eine Zerlegung von F.

Ist über dem Grundkörper keine solche Zerlegung möglich, so ist die Gruppe zweifach transitiv. Man wird nun eine Zerlegung im Körper $K(\sqrt{D})$ ansetzen, wo D die Diskriminante ist. Dabei ist die angegebene Methode etwas zu modifizieren: Die Faktoren von F müssen in $K(\sqrt{D})$ konjugiert sein, also die Form $P + Q\sqrt{D}$ und $P - Q\sqrt{D}$ haben. Ist nun d irgendein Primteiler von D so können wir auch mod d rechnen. Wir nehmen an, d sei der einzige Primfaktor, der in einer ungeraden Potenz in D aufgeht. Es ist $F \equiv p_0^2 \pmod{d}$. p_0 ist also, wenn überhaupt, dann leicht zu berechnen.

Bei beiden Moduln u und d besteht die Hauptschwierigkeit in der Berechnung des Anfangsgliedes der Entwicklung von Q. Dazu ist eine quadratische Kongruenz zu lösen. Man wird hier im allgemeinen nicht durchkommen, ohne eine gewisse Anzahl von Fällen durchzuprobieren. Wir arbeiten z.B. mit dem Modul d. Angenommen, wird könnten die ersten p_i und q_i berechnen, und es sei $q_h u^h$ das erste Glied in der Entwicklung von Q, das nicht identisch verschwindet. Wir setzen $\frac{1}{d}(F - p_0^2) = F_1$. Angenommen wir hätten $p_0, p_1,$

[3]) Grundzüge einer arithmetischen Theorie der algebraischen Größen. § 4 [Crelles J. **92** (1882)].

$\ldots, p_{i-1}$ $(i \leqq 2h+1)$ sowie $F_1, \ldots, F_{i-1}$ schon bestimmt, und es sei $F_{i-1} \equiv \sum_{\nu=0}^{i-1} p_\nu p_{i-1-\nu} \pmod d$. Wir setzen $\frac{1}{d}\left(F_{i-1} - \sum_{\nu=0}^{i-1} p_\nu p_{i-1-\nu}\right) = F_i$. Die Betrachtung der nächsten Glieder ergibt $F_i \equiv 2p_0 p_i + \sum_{\nu=1}^{i-1} p_\nu p_{i-\nu} \pmod d$. Wir setzen $G_i = F_i - \sum_{\nu=1}^{i-1} p_\nu p_{i-\nu}$ und errechnen p_i aus $2p_0 p_i \equiv G_i \pmod d$. So fortfahrend kommen wir zu der Kongruenz $F_{2h+1} \equiv 2p_0 p_{2h+1} + \sum_{\nu=1}^{2h} p_\nu p_{2h+1-\nu} - q_h^2 \pmod d$, also $q_h^2 \equiv -G_{2h+1} \pmod{p_0, d}$. Nun ist zwar mit Hilfe des quadratischen Reziprozitätsgesetzes[4]) leicht zu entscheiden, ob diese Kongruenz lösbar ist oder nicht. Die wirkliche Lösung kann aber erhebliche Schwierigkeiten machen. Ist p_0 ein Primpolynom vom Grade k, so können wir etwa das Galoisfeld heranziehen, dessen erzeugendes Element γ durch $p_0(\gamma) \equiv 0 \pmod d$ definiert ist. Es seien $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_k$ die verschiedenen Wurzeln von $p_0 \equiv 0 \pmod d$. Das primitive Element der multiplikativen Gruppe dieses Galoisfeldes sei δ. Dann können wir die Kongruenzen $q_h^2(\gamma_i) \equiv -G_{2h+1}(\gamma_i)$ aufstellen. Nun ist die Zahl $-G_{2h+1}(\gamma_i) = \delta^N$, da die multiplikative Gruppe immer zyklisch ist. Ist dabei d und N eine ungerade Zahl, so ist die Kongruenz unlösbar; ist N gerade, so ist $q_h(\gamma_i) \equiv \delta^{\frac{1}{2}N}$ zu setzen. Wenn wir die Werte von q_h an den k Stellen γ_i kennen, können wir mit Hilfe der Lagrangeschen Interpolationsformel $q_h(x)$ berechnen.

Bei den riesigen Galoisfeldern, die wir zu erwarten haben, wird aber das Auffinden der Zahl N im allgemeinen eine aussichtslose Aufgabe sein: Ist $f(x)$ vom 5. Grad, so ist $F(x)$ vom 20. Grad, p_0 vom 10. Grad und das Galoisfeld hat d^{10} Elemente. N müssen wir also durch Probieren aus den Zahlen $1, \ldots, d^{10}$ aussuchen. Die Aufgabe vereinfacht sich wesentlich, wenn p_0 kein Primpolynom ist.

Ist q_h bekannt, so setzen wir für $i > 2h+1$

$$\frac{1}{d}\left(G_{i-1} - 2p_0 p_{i-1} + 2q_h q_{i-h-2}\right) = F_i$$

$$F_i - \sum_{\nu=1}^{i-1} p_\nu p_{i-\nu} + \sum_{\nu=h+1}^{i-h-1} q_\nu q_{i-\nu-1} = G_i$$

und können, wenn p_0 und q_0 teilerfremd sind, q_{i-h} und p_i aus $2p_0 p_i - 2q_h q_{i-h} \equiv G_i \pmod d$ linear berechnen.

Unter der i-ten Stufe wollen wir dabei den Vergleich der Koeffizienten von d^i verstehen.

IV.

Als Anwendung stellen wir uns die Aufgabe, die Gleichung $x^5 + 5x^3 + 5x - 1 = 0$ zu behandeln, ihre Gruppe zu bestimmen, und wenn sich diese als auflösbar herausstellen sollte, die Gleichung aufzulösen.

a) Die Gleichung ist irreduzibel, wie man nach der Substitution $x = y + 1$ nach Eisenstein leicht sieht.

b) Die Diskriminante der Gleichung ist 5^7, wie eine kurze Rechnung zeigt.

[4]) HASSE: Zahlentheorie, § 5g, S. 72. 1949.

c) Die Gleichung gestattet in Restklassenkörpern bzw. in den zugehörigen durch die Gleichung $x^2 + x - 1 = 0$ definierten Galoisfeldern folgende Zerlegungen in Primfaktoren; wenn ϱ und $\bar{\varrho}$ die Wurzeln von $x^2 + x - 1 \equiv 0$ sind:

$$f(x) \equiv (x+1)(x^4+x^3+1) \pmod 2$$
$$\equiv (x+1)(x^2+\varrho x+\varrho)(x^2+\bar{\varrho}x+\bar{\varrho})$$
$$f(x) \equiv (x+1)(x^4-x^3-1) \pmod 3$$
$$\equiv (x+1)(x^2+\varrho x+1+\varrho)(x^2+\bar{\varrho}x+1+\bar{\varrho})$$
$$f(x) \equiv (x-1)^5 \pmod 5$$
$$f(x) \equiv (x-3)(x^4+3x^3+5) \pmod 7$$
$$\equiv (x-3)(x^2-3\varrho x+5+\varrho)(x^2-3\bar{\varrho}x+5+\bar{\varrho})$$

$f(x)$ ist irreduzibel (mod 11).

Die Gruppe enthält also sicher einen Fünfer- und einen Viererzyklus, ihr alternierender Normalteiler ein Paar von Zweierzyklen[5]). Es kommen also nur die volle symmetrische und die volle metazyklische Gruppe in Betracht. Eine Entscheidung zwischen ihnen können wir durch Betrachtung von Kongruenzen nicht erreichen.

d) Es ist $g(x;\alpha) = x^4 + \alpha x^3 + (\alpha^2+5)x^2 + (\alpha^3+5\alpha)x + \alpha^4 + 5\alpha^2 + 5$. Die kleinste Zahl, die nicht in der Diskriminante aufgeht, ist 2; wir berechnen

$$g(x-2\alpha;\alpha) = 11\alpha^4 - 23\alpha^3 x + \alpha^2(19x^2+15) + \alpha(-7x^3-15)x + x^4 - 5x^2 - 5.$$

Die Norm $N(g(x-2\alpha;\alpha))$ finden wir, indem wir $g(x-2\alpha;\alpha)$ nacheinander mit $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ multiplizieren, mod $f(\alpha)$ auf Polynome 4. Grades reduzieren und die Determinante der Koeffizienten der verschiedenen Potenzen von α bilden. Es wird $N(g(x-2\alpha;\alpha)) =$

11	$-23x$	$19x^2+15$	$-7x^3-15x$	x^4+5x^2+5
$-23x$	$19x^2-40$	$-7x^3-15x$	x^4+5x^2-50	11
$19x^2-40$	$-7x^3+100x$	x^4+5x^2-50	$115x+11$	$-23x$
$-7x^3+100x$	x^4-90x^2+150	$115x+11$	$-95x^2-23x+200$	$19x^2-40$
x^4-90x^2+150	$35x^3-385x+11$	$-95x^2-23x+200$	$35x^3+19x^2-500x-40$	$-7x^3+100x$

Bei der Berechnung dieser Determinante kann man mit Hilfe des Laplaceschen Satzes nach den Elementen der beiden ersten und der drei letzten Spalten entwickeln. Andere Determinantensätze heranzuziehen scheint sich nicht zu lohnen. Die Rechnung ist im Prinzip einfach, aber freilich etwas umfangreich. Wir erhalten

$$N(g(x-2\alpha;\alpha)) = F(x)$$
$$= x^{20} + 80x^{80} + 2570x^{16} + 78x^{15} + 43200x^{14} + 3930x^{13} + 417275x^{12} +$$
$$+ 72420x^{11} + 2418344x^{10} + 652050x^9 + 8532510x^8 + 3080100x^7 +$$
$$+ 18139840x^6 + 7500972x^5 + 22191925x^4 + 8767440x^3 +$$
$$+ 13438600x^2 + 4341810x + 2328551.$$

[5]) Waerden, van der: Moderne Algebra I, 1. Aufl., § 56, S. 188. 1930.

e) Die Kongruenzen unter c) zeigen, daß mit einer Zerlegbarkeit im rationalen Zahlkörper nicht zu rechnen ist, wohl aber im Körper $K(\sqrt{5})$ und dann notwendig in Polynome gleichen Grades der Form $F=(P'+\varrho Q')\,(P'+\bar{\varrho} Q')$, wo ϱ und $\bar{\varrho}$ die Wurzeln von $x^2+x-1=0$, nämlich $\varrho, \bar{\varrho}=\frac{-1\pm\sqrt{5}}{2}$ sind. Weil $F(x)$ mit $1\cdot x^{20}$ beginnt, dürfen wir annehmen, daß beide Faktoren mit $1\cdot x^{10}$ beginnen, daß also Q keine Glieder 10. Ordnung enthält. Das Kroneckersche Verfahren ist hier überhaupt nicht unmittelbar anzuwenden, weil der Körper unendlich viele Einheiten, jede Zahl also unendlich viele Faktoren hat.

Nach III. haben wir mod 2 die Zerlegung $F(x)=(x^5+x^3+x+1)^4$ zu erwarten. Sie ist in der Tat eine mögliche Zerlegung. Also sind alle Koeffizienten von Q' gerade und wir können in Zukunft $\sqrt{5}$ an Stelle von ϱ als Glied der Körperbasis wählen. Damit rechnet sich einfacher. Wir suchen also eine Zerlegung $F=(P+Q\sqrt{5})\,(P-Q\sqrt{5})$, wo $P=P'-\frac{Q'}{2}$, $Q=\frac{Q'}{2}$. Die weitere Rechnung mod 2 hat zwei Nachteile: Erstens geht sie sehr langsam und zweitens wird das Verfahren mod 8 nicht mehr linear: Wir erhalten

$$F\equiv p_0^2+4p_1p_0+4p_1^2-q_0^2-4q_1q_0-q_1^2 \pmod 8,$$

und dies ist eine Kongruenz 2. Grades für p_1 und q_1. Die Rechnung wurde deshalb 5-adisch weitergeführt. Wir berechnen p_0 aus der Kongruenz $p_0^2=F \pmod 5$ zu $p_0=(x^5+2)^2\equiv(x+2)^{10} \pmod 5$. Das ist außerordentlich günstig für die Lösung der quadratischen Kongruenz für das Anfangsglied der Entwicklung von Q. Da wir häufig durch p_0 zu dividieren haben, läge es nahe, $F(x)$ durch $x=y-2$ in die Form $F(y)$ zu transformieren. Jedoch ist die Umrechnung eines Polynoms 20. Grades rechnerisch nicht in wenigen Augenblicken durchzuführen und führt zu Koeffizienten der Größenordnung 10^{11} und 10^{12}, mit denen man auf den üblichen Rechenmaschinen nicht mehr alle Operationen ohne weiteres ausführen kann. Wir verzichten daher darauf und transformieren dafür lieber jedes $G_i(x)$ für sich mod 5 in $G_i^*(y)$. Diese Rechnung ist jedesmal in wenigen Zeilen durchzuführen. Wir geben nun eine Tabelle der $G_i^*(y)$. Wir müssen dabei für jedes i eine bestimmte vorläufige Lösung der p_ν und q_ν zugrunde legen. Im weiteren Verlauf der Rechnung werden wir noch zu Korrekturen gezwungen und legen demzufolge andere vorläufige Lösungen zugrunde. Es ist also

	y^{19}	y^{15}	y^{10}	y^5	y^0
G_1^*	. 1 4 1 3	. . . . .	. . . . .	. . . . .	
G_2^*	. 2 3 2 .	1 . 3 1 2	. . . . .	. . . . .	
G_3^*	. . . 1 3	4 4 3 1 .	. . . . .	. . . . .	
G_4^*	. . . . .	1 2 2 3 4	. . . . .	. . . . .	
G_5^*	. . . . .	 3	. . . . .	. . . . .	
G_6^*	. . . . .	 1	. 2 3 . .	. . . . .	
G_7^*	. . . . .	. . . 2 4	1 2 2 4 1	. . .	
G_8^*	. . . . .	 1	1 3 4 4 .	4 2 . . .	
G_9^*	. . . . .	 1	3 3 3 1 1	. . . . .	
G_{10}^* bis G_{19}^*	. . .	. . . . .	. . . . .	. . . . .	

Aus den Kongruenzen ergeben sich daraus für p_i und q_i

x^{10}				x^5					x^0	
p_0 1	.	.	.	.	4	.	.	.	.	4	
p_1 .	.	3	.	2	2	.	1	.	4	4	
p_2 .	.	1	.	4	1	3	1	1	3	3	
p_3 .	.	.	.	3	.	2	3	4	3	.	$+2r_1^2$
p_4 .	.	.	.	.	.	3	.	4	1	.	$+4r_1r_2$
p_5 .	.	.	.	.	.	.	.	.	.	4	$+4r_1r_3+2r_2^2$
p_6 .	.	.	.	.	.	.	.	.	.	3	$+4r_2r_3+2r_1r_4$
p_7 .	.	.	.	.	.	.	.	.	−4	2	$+2r_2r_4+2r_3^2+2(x+1)r_5+(-4x+5)s$
p_8 .	.	.	.	.	.	.	.	.	.	−2	$+4xr_4+3r_5+2(x+1)r_6$
p_9 .	.	.	.	.	.	.	.	.	.	1	$+2(x+1)r_7$
q_1						.	.	.	.	.	$(x^5+2)2r_1$
q_2						.	.	.	.	.	$A_1r_1+2(x^5+2)r_2$, wo $A_1=3x^3+2x+2$
q_3						.	.	.	.	.	$A_2r_1+A_1r_2+2(x^5+2)r_3$, wo $A_2=x^3+3x+1$
q_4						1	5	13	19	7	$+A_1r_3+(x^5+2)r_4$
q_5						.	.	1	−1	1	$+A_2r_3-2A_1r_4+(x+2)^3r_5+(x^3+7x^2+10x+7)s$
q_6						.	.	1	4	4	$+(4x^3+2x^2+4x)r_4+(2x+4)r_5+(x+2)^3r_6$
q_7						.	.	2	4	3	$+(x+2)^3r_7$

Bei der Suche nach der allgemeinen Lösung der 1-ten Stufe müssen wir die Kongruenz $q_0^2 = 0 \pmod{5, p_0}$ lösen. Sie ergibt $q_0 = (x^5+2)\,2r_0$. Zur Bestimmung von r_0 erweist sich eine Fallunterscheidung als notwendig nach der Potenz von y, durch die dieses r_0 als teilbar angenommen wird. Die Potenzen y^0 und y^1 erweisen sich bereits auf der zweiten Stufe als unmöglich, y^2 als auf der dritten, y^3 und y^4 auf der vierten. Wir müssen also mit $r_0 = 0$ weiterrechnen. Auf der dritten Stufe stehen wir wieder vor der Kongruenz $q_1^2 = 0 \pmod{5, p_0}$ mit der allgemeinen Lösung $q_1 = (x^5+2)\,2r_1$. Auf jeder folgenden Stufe wurde dann eine Partikularlösung berechnet und jedesmal die allgemeine Lösung der homogenen Kongruenz

$$2(x^5+2)^2 p_{i+1} - 4(x^5+2)\,r_1\,q_i \equiv 0 \pmod 5$$

mit unbestimmten r_i hinzugefügt. Bei den ersten Stufen wurde zunächst einmal versuchsweise auf die volle Allgemeinheit verzichtet und außer acht gelassen, daß r_1 und p_0 noch einen Faktor gemein haben können. Erst nachdem sich auf der 6. Stufe herausgestellt hat, daß auch r_1 durch y^2 teilbar ist, wurde dies berücksichtigt. Zu den G_i treten dann noch gewisse Ausdrücke, die sich aus den r_i zusammensetzen. Diese unbestimmten Polynome r_i lassen sich dann auf den höheren Stufen aus der Bedingung berechnen, daß G_i durch den größten gemeinsamen Teiler von $r_1(x^5+2)$ und p_0 teilbar sein muß, wenn die Kongruenzen überhaupt noch Lösungen haben sollen.

Auf der 6. Stufe ergab sich die Kongruenz $y^{10} + 2y^8 + 3y^7 \equiv G_6 = -4q_1q_4 + 2p_0p_6 + r_1^2y^4 + 4r_1^4 + 4A_1r_1r_3y^5 + 4A_2r_1r_2y^5 - 8r_2r_3y^{10} \pmod 5$. Daraus können wir schließen, daß r_1 genau durch y^2 teilbar ist. Im übrigen ist die Kongruenz von r_1 im 4. Grad, und wir werden sie nicht in allgemeinen Buchstaben lösen können, sondern wir werden für r_1 verschiedene Ansätze durchprobieren

müssen. Am nächsten liegt wohl der, daß die Glieder unter y^{10} für sich durch r_1 teilbar sind, daß also $r_1 = \lambda(2y+3)y^2$. Auf der 7. Stufe findet man dann $\lambda^2 = 4$. Wir können uns willkürlich für eine der beiden Wurzeln, etwa für $\lambda = 3$ entscheiden; $\lambda = 2$ liefert den anderen Faktor der Zerlegung von F. Wir setzen dementsprechend $r_1 = (x+1)(x+2)^2$. Die weitere Rechnung verläuft nun linear. Auf der 7. Stufe finden wir $r_2 = 4x + 1 + sy^2$; die 8. Stufe liefert $s = 4$. Unter den Repräsentanten der entsprechenden Restklassen wählen wir $r_2 = -x^2 - 3$. Auf der 8. Stufe findet man noch $r_3 = -2 - r_5$, auf der 9. Stufe $r_3 = -2$, $r_4 = 1$, $r_5 = 0$, $r_6 = -2$. Die Repräsentanten der Restklassen sind dabei so gewählt, daß jedesmal die höchsten Glieder von $G_i(x)$ auf beiden Seiten gleich und nicht nur (mod 5) kongruent werden.

Beim Weiterrechnen werden alle $G_i = 0$ $(i \geqq 10)$ und F_{19} verschwindet, wenn wir alle r_i $(i \geqq 7)$ durch Null ersetzen. Wir haben also eine Zerlegung $F = (P + Q\sqrt{5})(P - Q\sqrt{5})$, wobei

$$P = x^{10} + 40x^8 + 735x^6 + 39x^5 + 6200x^4 + 2555x^3 + 19025x^2 + \\ + 7095x + 20974$$

$$Q = 10x^8 + 280x^3 + 15x^5 + 2650x^4 + 495x^3 + 8400x^2 + 3135x + 9355.$$

f) Wir haben nun den größten gemeinsamen Teiler von $(P + Q\sqrt{5})$ mit $g(x - 2\alpha; \alpha)$ zu suchen. Wir werden dabei $\sqrt{5}$ wieder durch $2\varrho + 1$ mit $\varrho = \frac{-1+\sqrt{5}}{2}$ ersetzen müssen. Mit Hilfe des Euklidischen Algorithmus finden wir nach zwei Divisionen für diesen größten gemeinsamen Teiler das Polynom

$$x^2 - (4 + \varrho)\alpha x + \alpha^2(5 + 2\varrho) + 3 + \varrho,$$

also, wenn wir $x - 2\alpha$ wieder durch x ersetzen

$$g(x) = (x^2 - \varrho\alpha x + \alpha^2 + 3 + \varrho)(x^2 - \bar{\varrho}\alpha x + \alpha^2 + 3 + \bar{\varrho}) = g_1 g_2 \text{ [6]}.$$

g) Die Zerlegung aus f) zeigt uns, daß die Gruppe von $f(x)$ nicht die symmetrische, sondern die volle metazyklische ist. Es sei β eine Wurzel von g_1; dann ist $\varrho\alpha - \beta$ die andere Wurzel. Da es nun keine Permutation der Wurzeln von $f(x)$ geben kann, die α und die Wurzeln von g_1 festläßt, die von g_2 aber vertauscht, muß g_2 bei Adjunktion von β zerfallen. Um die Faktorzerlegung zu finden, überzeugen wir uns zunächst davon, daß es ein Element der Gruppe gibt, das α und β vertauscht. In der Tat gibt es Gruppenelemente mit Zweierzyklen und wegen der Transitivität auch ein solches, das α mit einer anderen Wurzel γ vertauscht. Ist γ eine Wurzel von g_1 so sind wir fertig. Ist γ eine Wurzel von g_2, so beachten wir, daß es einen Automorphismus des Körpers

[6]) Dieses Ergebnis hätten wir auch bekommen, wenn wir für $g(x; \alpha)$ eine Zerlegung in den beiden Unbestimmten x und α angesetzt hätten. In unserem speziellen Beispiel hat sich also der Weg über die Norm als Umweg erwiesen.

gibt, bei dem $\sqrt{5} \to -\sqrt{5}$, $g_1 \to g_2$, $\alpha \to \alpha$, $\gamma \to \beta$. Also gibt es ein Gruppenelement, das den Zweierzyklus $(\alpha\beta)$ enthält. Dieses Element führt $\varrho\alpha - \beta$ in $\varrho\beta - \alpha$ über.

$\varrho\beta - \alpha$ ist von α, β und $\varrho\alpha - \beta$ verschieden, weil sich sonst eine lineare Beziehung zwischen α und β ergeben würde, während g_1 doch irreduzibel ist. Also ist $\varrho\beta - \alpha$ die eine Wurzel von g_2; $-\varrho(\alpha + \beta)$ ist dann die andere. Die Wurzeln 1. α, 2. β, 3. $\varrho\alpha - \beta$, 4. $-\varrho(\alpha + \beta)$, 5. $\varrho\beta - \alpha$ gestatten offensichtlich die Permutationen (12) (35) und (23) (45). Diese erzeugen die alternierende Untergruppe der metazyklischen Gruppe. Jetzt liefern die bekannten Methoden[7]) die Wurzeln $\alpha_\nu = \varepsilon^\nu \sqrt[5]{\frac{1+\sqrt{5}}{2}} + \varepsilon^{5-\nu} \sqrt[5]{\frac{1-\sqrt{5}}{2}}$ ($\nu = 0, 1, 2, 3, 4$ und $\varepsilon^2 = 1$).

[7]) Perron: Algebra II, 2. Aufl., § 43, S. 226. 1933.

Halle, Mathematisches Institut der Universität.

(Eingegangen am 26. Februar 1955.)

TAUSSKY, O.
Math. Zeitschr. Bd. 63, S. 286—289 (1955)

Unimodular integral circulants*.

In memoriam ISSAI SCHUR.

By

OLGA TAUSSKY.

Some properties of the "discriminant matrix" $(\alpha_i^{(S_k)})$ of a normal algebraic number field of degree n were investigated in two previous notes (1,2). Here the α_i form an integral basis of the field and the S_k are the elements of the GALOIS group[1]). In the special case when the α_i form a normal basis various problems concerning group matrices arise, among others, questions concerning unimodular group matrices whose elements are rational integers. If the field is cyclic circulant[2]) matrices appear, i.e. matrices $C = (c_{ik})$ with $c_{ik} = c_{k-i+1}$ where the suffixes are considered mod n. In particular the following theorem was obtained which will be studied further in the present note:

Theorem 1. *Let C be a unimodular circulant of rational integers of the form AA' where A is a unimodular matrix of rational integers. Let C be an $n \times n$ matrix. Then A is the product of a circulant, a permutation matrix and a diagonal matrix whose elements are ± 1.*

Now let $n = p$ be (in particular) a prime and $B = (b_{k-i+1})$ a unimodular circulant[3]). Since B is unimodular, we have

$$b_1 + \cdots + b_p = \pm 1$$
$$b_1 + b_2\zeta + \cdots + b_p\zeta^{p-1} = \varepsilon_B$$

where ε_B is a unit in the field $F(\zeta)$ generated by ζ, a p-th root of unity.

We first prove two lemmas which are concerned with these units which are "associated" with unimodular circulants.

Lemma 1. *Let B be a unimodular circulant and ε_B its associated unit. Then BB' has $\varepsilon_B \bar{\varepsilon}_B$ as its associated unit.*

Proof. Since the associated unit is also an eigenvalue and since circulants are polynomials in the permutation matrix, the statement follows at once.

It is convenient to consider the product $\varepsilon\bar{\varepsilon}$ as the norm of ε with respect to the field $F(\zeta + \zeta^{-1})$.

A converse of Lemma 1 is:

*) This work was supported (in part) by the Office of Naval Research.

[1]) The idea of studying discriminant matrices was suggested by I. SCHUR's treatment of GAUSS sums; see E. LANDAU, Vorlesungen über Zahlentheorie, Leipzig 1927, p. 162—166.

[2]) For a detailed study of circulants see e.g. (3).

[3]) In what follows all circulants are assumed to have rational integers as elements.

Lemma 2. *Let C be a unimodular circulant and assume that its associated unit $\varepsilon_C = \varepsilon\,\bar{\varepsilon}$, where ε is the unit $b_1 + b_2\zeta + \cdots + b_p\zeta^{p-1}$. Then $C = BB'$ where B is the circulant whose first row is $b_1, b_2, \ldots, b_p$.*

Proof. Consider the equation

$$c_1 + c_2\zeta + \cdots + c_p\zeta^{p-1} = (b_1 + b_2\zeta + \cdots + b_p\zeta^{p-1})(b_1 + b_2\zeta^{-1} + \cdots + b_p\zeta^{-(p-1)}).$$

Since the expansion in powers of ζ is unique, we obtain by comparing coefficients

$$\begin{aligned}
c_1 &= b_1^2 + b_2^2 + \cdots + b_p^2\\
c_2 &= b_1 b_p + b_2 b_1 + \cdots + b_p b_{p-1}\\
c_3 &= b_1 b_{p-1} + b_2 b_p + \cdots + b_p b_{p-2}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
c_p &= b_1 b_2 + b_2 b_3 + \cdots + b_p b_1.
\end{aligned}$$

From this $C = BB'$ follows by inspection.

From Lemmas 1, 2 and Theorem 1 we conclude:

Theorem 2. *Let $C = AA'$ be a unimodular circulant where A is a unimodular matrix with rational integers as elements. Then the unit ε_C associated with C is the norm of a unit ε of $F(\zeta)$ with respect to $F(\zeta + \zeta^{-1})$. If $\varepsilon = b_1 + b_2\zeta + \cdots + b_p\zeta^{p-1}$ then $C = BB'$ where B is the circulant whose first row is $(b_1, \ldots, b_p)$.*

We will now prove a special instance of Theorem 2 (for $p = 5$) without explicitly using the fact that the matrix is of the form AA'.

Theorem 3. *Let C be a symmetric and positive definite unimodular 5×5 circulant. Then ε_C is the norm of a unit of $F(\zeta)$ with respect to $F(\zeta + \zeta^{-1})$ where ζ is a 5-th root of unity.* (By Lemma 2 this implies that $C = BB'$ where B is a circulant derived from the unit.)

Proof of Theorem 3[4]).

Let c_1, c_2, c_3, c_4, c_5 be the elements of the first row of C. Since C is symmetric, we have

$$c_2 = c_5,\quad c_3 = c_4.$$

We have therefore the relation

$$c_1 + 2c_2 + 2c_3 = \pm 1.$$

The value -1 is not possible since the determinant of C is $+1$ by assumption and since its value is the product of $c_1 + 2c_2 + 2c_3$ and the norm of a unit in $F(\zeta)$. This norm must have the value $+1$ since the field is complex. We further know that

$$c_1 + c_2\zeta + c_3\zeta^2 + c_3\zeta^3 + c_2\zeta^4 = \varepsilon$$

where ε is a unit in the field $F(\zeta)$. From the special form of ε it is evident that it lies in the quadratic subfield generated by $\eta = \zeta + \zeta^{-1}$ which is the

[4]) I am indebted to J. Todd for some helpful suggestions.

field generated by $\sqrt{5}$. We now show that ε is the norm of a unit of $F(\zeta)$ with respect to $F(\eta)$. For this purpose we show that ε is the square of another unit in $F(\eta)$. The field $F(\eta)$ has η as a fundamental unit. What we are going to prove is that

$$\varepsilon = c_1 - c_3 + (c_2 - c_3)\eta \tag{1}$$

is an even power of η under the assumption that

$$c_1 + 2c_2 + 2c_3 = 1. \tag{2}$$

We start by showing some simple facts about the powers of η. The number η satisfies the equation

$$x^2 + x - 1 = 0.$$

From this it follows easily (e.g. by induction) that in

$$\eta^n = x_n + y_n\eta$$

the product

$$x_n y_n < 0, \quad n > 1, \tag{3}$$

in particular:

$$\begin{aligned} &x_n > 0,\ y_n < 0,\ n \text{ even}, > 0 \\ &x_n < 0,\ y_n > 0,\ n \text{ odd}, > 1. \end{aligned} \tag{4}$$

From the positive definiteness of C it follows that

$$c_1 > 0. \tag{5}$$

We next show that

$$c_1 - c_3 > 0. \tag{6}$$

For, if $c_1 - c_3 < 0$, then $c_3 > 0$, hence from (2) we have $c_2 < 0$, which implies $c_2 - c_3 < 0$. This would imply that the coordinates in (1) are of the same sign which contradicts (3). Hence (6) holds because $c_1 - c_3 = 0$ implies $c_2 - c_3 = \pm 1$ in view of (1). This, however, contradicts (2).

From (4) it follows that (1) is an even power of η or the negative of an odd power. We now show that the latter is not true: for, it follows from (2) that

$$c_1 + 2c_2 + 2c_3 = (c_1 - c_3) + 2(c_2 - c_3) + 5c_3 = 1,$$

hence

$$c_1 - c_3 + 2(c_2 - c_3) \equiv 1\ (5). \tag{7}$$

So we have to show that

$$x_n + 2y_n \equiv 1\ (5) \tag{8}$$

cannot happen for $-\eta^n$, n odd.

We will even show that $x_n + 2y_n \not\equiv \pm 1 (5)$ for n odd, $n > 1$. This can again be shown by induction: for $n = 3$ we have

$$\eta^3 = -1 + 2\eta,$$

hence the assertion is true for $n = 3$. Putting again

$$\eta^n = x_n + y_n \eta,$$

it follows that

$$x_{2n+3} + 2y_{2n+3} = -x_{2n+1} + 3y_{2n+1} \equiv -(x_{2n+1} + 2y_{2n+1}) (5),$$

hence (8) cannot happen for n odd.

We have now shown that ε is an even power of η, hence it is the norm of a unit in $F(\eta)$.

References.

[1] Taussky, O.: Normal matrices in some problems in algebraic number theory. Proc. Internat. Congr. Math., Amsterdam, 1954. — [2] Newman, M., and O. Taussky: On a generalization of the normal basis in abelian algebraic number fields. To appear in Comm. Pure Appl. Math. — [3] Hamburger, H. L., and M. E. Grimshaw: Linear Transformations, Cambridge 1951, pp. 94—96.

National Bureau of Standards, Washington, D. C. (USA).

(Eingegangen am 7. März 1955)

Hirsch, K. A.
Math. Zeitschr. Bd. 63, S. 290—294 (1955)

Über lokal-nilpotente Gruppen.

Issai Schur zum Gedächtnis.

Von

Kurt A. Hirsch.

An anderer Stelle ([8], [9]) habe ich den folgenden Satz bewiesen:

Satz 1. *Eine Gruppe G mit Maximalbedingung für Untergruppen, in der jede echte Untergruppe von ihrem Normalisator verschieden ist, ist nilpotent*[1]).

Es liegt nahe, zu fragen, ob die Voraussetzung der Maximalbedingung abgeschwächt oder ganz fortgelassen werden kann, wenn die Folgerung entsprechend abgeschwächt wird. In dieser Richtung hat Plotkin den folgenden Satz bewiesen ([11]; s. auch [10], § 62):

Satz 2. *Eine Gruppe G, in der jede echte Untergruppe von ihrem Normalisator verschieden ist, ist lokal-nilpotent*[2]).

Ich will nun hier zeigen, daß eine verschärfte Form der Schlüsse, die ich bei dem Beweis von Satz 1 benutzt habe, ausreicht, um einen einfachen Beweis von Satz 2 zu erbringen. Zu diesem Zweck brauche ich zwei Sätze, die auch an sich Interesse beanspruchen dürfen.

Satz 3. *Jede beliebige Gruppe G besitzt einen eindeutig bestimmten maximalen lokal-nilpotenten Normalteiler, der alle lokal-nilpotenten Normalteiler von G umfaßt.*

Dieser Satz ist eine unmittelbare Folge von

Satz 4. *Das Erzeugnis zweier lokal-nilpotenter Normalteiler A und B einer beliebigen Gruppe G ist selbst lokal-nilpotent.*

Satz 4 und Satz 3 entsprechen den beim Beweis von Satz 1 benutzten Tatsachen, daß das Erzeugnis zweier nilpotenter Normalteiler einer beliebigen Gruppe selbst ein nilpotenter Normalteiler ist, und daß daher jede Gruppe mit Maximalbedingung für Normalteiler einen eindeutigen maximalen nilpotenten Normalteiler besitzt, der alle nilpotenten Normalteiler umfaßt ([7], Theorem 3.1; s. auch [2], Satz 14).

Schließlich will ich noch auf ein mehrfach zu benutzendes Korollar eines Satzes von Baer hinweisen ([1], S. 363; s. auch [10], § 63):

Satz 5. *Jede endlich erzeugte nilpotente Gruppe erfüllt die Maximalbedingung für Untergruppen.*

[1]) Eine Gruppe heißt nilpotent, wenn sie eine Zentralreihe endlicher Länge besitzt.
[2]) Lokal-nilpotent heißt eine Gruppe, in der jedes endliche System von Elementen eine nilpotente Untergruppe erzeugt.

Beweis von Satz 4. 1. A und B seien zwei lokal-nilpotente Normalteiler einer Gruppe G. Wenn a und b zwei beliebige Elemente von A und B sind, so liegt der Kommutator $a' = [a, b] = b'$ sowohl in A als auch in B. Nun ist die Gruppe $\{b', b\}$ als endlich erzeugte Untergruppe von B nach Voraussetzung nilpotent, so daß wir bei genügender Wiederholung der Kommutatorbildung $[b', b, b, \ldots, b] = 1$ erhalten. Wegen $b' = a'$ besagt dies: Setzen wir $[a, b] = a'$, $[a', b] = a''$ und so weiter, so bricht die Folge $a, a', a'', \ldots$ nach endlich vielen Schritten mit dem Einheitselement ab.

2. Um zu zeigen, daß $\{A, B\}$ lokal-nilpotent ist, nehmen wir in $\{A, B\}$ ein beliebiges endliches System von Elementen, das wir in der Form $a_1 b^{(1)}$, $a_2 b^{(2)}, \ldots, a_n b^{(n)}$ schreiben wollen. Wir werden die Gruppe $\{a_1 b^{(1)}, a_2 b^{(2)}, \ldots, a_n b^{(n)}\}$ dadurch als nilpotent erweisen, daß wir sie in eine nilpotente Untergruppe von $\{A, B\}$ einbetten. Wir setzen $A_0 = \{a_1, a_2, \ldots, a_n\}$ und $B^* = \{b^{(1)}, b^{(2)}, \ldots, b^{(n)}\}$. Als endlich erzeugte Untergruppe von B ist B^* nilpotent und erfüllt nach Satz 5 die Maximalbedingung für Untergruppen. Also hat B^* (s. [6], Theorem 2.311) eine „Hauptreihe"

$$\{1\} = B_0 < B_1 < B_2 < \cdots < B_k = B^*, \tag{1}$$

in der die Gruppen B_i $(i = 1, 2, \ldots, k)$ Normalteiler von B^* sind und B_{i+1}/B_i eine zyklische Gruppe (von endlicher oder unendlicher Ordnung) ist. Es sei b_i, $i = 1, 2, \ldots, k$, ein Vertreter eines erzeugenden Elementes von B_i/B_{i-1} in B^*, so daß insbesondere $\{b_1, b_2, \ldots, b_i\} = B_i$ ist.

3. Wir konstruieren jetzt für jedes i $(i = 1, 2, \ldots, k)$ eine Gruppe A_i, die den folgenden Bedingungen genügt:

(i) A_i ist eine endlich erzeugte Untergruppe von A, die A_0 umfaßt.

(ii) In der aufsteigenden Folge

$$A_i < \{A_i, B_1\} < \{A_i, B_2\} < \cdots < \{A_i, B_i\} \tag{2}$$

ist jedes Glied Normalteiler des darauffolgenden, und alle Glieder sind nilpotent.

Wir beginnen mit $i = 1$. Wenn wir den unter 1. beschriebenen Prozeß der wiederholten Kommutatorbildung mit b_1 auf alle erzeugenden Elemente von A_0 anwenden, erhalten wir

$$a_1, a_1', a_1'', \ldots; \quad a_2, a_2', a_2'', \ldots; \quad \ldots; \quad a_n, a_n', a_n'', \ldots. \tag{3}$$

A_1 sei die von all diesen endlich vielen Elementen erzeugte Gruppe. Als endlich erzeugte Untergruppe von A ist A_1 nilpotent. Ferner ist A_1 Normalteiler von $\{A_1, B_1\}$, da ja für jedes Element a_m, $m = 1, 2, \ldots, n$

$$b_1^{-1} a_m^{(j)} b_1 = a_m^{(j)} a_m^{(j+1)} \in A_1 \tag{4}$$

ist. Wir zeigen nun, daß $\{A_1, B_1\}$ wiederum nilpotent ist. Als nilpotente Gruppe hat A_1 ein nicht-triviales Zentrum Z. Sei $z \neq 1$ ein beliebiges Element von Z. Wenn nicht schon $[z, b_1] = 1$ ist, so formen wir, wie oben, durch wiederholte Kommutatorbildung $z, z', z'', \ldots$ und kommen nach endlich vielen

Schritten zu einem Zentrumselement von A_1, das auch mit b_1 vertauschbar ist, also zum Zentrum von $\{A_1, B_1\}$ gehört. Wir bilden nun die Faktorgruppe nach diesem Zentrum und sehen durch vollständige Induktion, daß $\{A_1, B_1\}$ nilpotent ist.

4. Im allgemeinen Fall sei die Gruppe A_i folgendermaßen definiert. Wir nehmen die erzeugenden Elemente a_m $(m = 1, 2, \ldots, n)$ von A_0 und fügen alle diejenigen Elemente von A hinzu, die durch wiederholte Kommutatorbildung mit b_i entstehen; dann weiter die wiederholten Kommutatoren all dieser Elemente mit b_{i-1}; in dieser Weise fahren wir mit $b_{i-2}, b_{i-3}, \ldots, b_1$ fort. Die erzeugenden Elemente von A_i sind also die a_m $(m = 1, \ldots, n)$ und alle Kommutatoren der Form

$$a = [a_m, b_{\alpha_1}, b_{\alpha_2}, \ldots, b_{\alpha_s}] \tag{5}$$

wobei $i \geqq \alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_s \geqq 1$ ist.

Auf Grund der Bemerkung unter 1. gibt es nur endlich viele verschiedene Kommutatoren dieser Form, so daß die Forderung (i) für A_i erfüllt ist.

Daß nun A_i Normalteiler von $\{A_i, B_1\}$ und die letztere Gruppe nilpotent ist, sehen wir genau wie unter 3. Nehmen wir schon als bewiesen an, daß die Forderung (ii) in der Folge (2) bis zu $\{A_i, B_{j-1}\}$ erfüllt ist. Dann haben wir zu zeigen, daß $\{A_i, B_{j-1}\}$ Normalteiler von $\{A_i, B_j\} = \{A_i, B_{j-1}, b_j\}$ ist. Nun ist B_{j-1} Normalteiler von B_j. Es genügt also zu zeigen, daß für jeden Kommutator (5)

$$b_j^{-1} a b_j \in \{A_i, B_{j-1}\} \tag{6}$$

gilt.

Es sei r so bestimmt, daß $\alpha_r \geqq j > \alpha_{r+1}$ ist. Dann setzen wir

$$[a_m, b_{\alpha_1}, b_{\alpha_2}, \ldots, b_{\alpha_r}] = \bar{a},$$

wobei $\bar{a}$ wieder ein erzeugendes Element von A_i ist. Wir haben also

$$b_j^{-1} a b_j = b_j^{-1} [\bar{a}, b_{\alpha_{r+1}}, \ldots, b_{\alpha_s}] b_j = [b_j^{-1} \bar{a} b_j, b_j^{-1} b_{\alpha_{r+1}} b_j, \ldots, b_j^{-1} b_{\alpha_s} b_j]. \tag{7}$$

Hierin ist $b_j^{-1} \bar{a} b_j = \bar{a} [\bar{a}, b_j]$ ein Produkt von zwei Erzeugenden von A_i, und alle übrigen Elemente der Klammer liegen in B_{j-1}, da $\alpha_{r+1} \leqq j - 1$ und B_{j-1} Normalteiler von B_j ist. Damit ist (6) bewiesen. Tatsächlich läßt sich aber viel mehr zeigen, nämlich daß A_i Normalteiler in $\{A_i, B_j\}$ ist. Denn wir können mit Hilfe der fundamentalen Kommutator-Identitäten

$$\begin{cases} [a b, c] = b^{-1} [a, c] b [b, c] = [a, c] [a, c] [a, c, b] [b, c] \\ [a, b c] = [a, c] c^{-1} [a, b] c = [a, c] [a, b] [a, b, c] \end{cases} \tag{8}$$

die rechte Seite von (7) sukzessiv so umformen, daß ein Produkt von Elementen der Form (5) entsteht. Hierzu stellen wir für jedes $\alpha \leqq \alpha_{r-1}$ das Element $b_j^{-1} b_\alpha b_j$ in der Form

$$b_j^{-1} b_\alpha b_j = b_\alpha b_\beta b_\gamma \ldots b_\omega \tag{9}$$

dar, mit $\alpha \geqq \beta \geqq \gamma \geqq \cdots \geqq \omega \geqq 1$, was in einer nilpotenten Gruppe stets möglich ist. Die etwas langwierigen Einzelheiten des Beweises brauchen hier nicht durchgeführt zu werden.

Die Nilpotenz von $\{A_i, B_j\}$ ergibt sich aus der von $\{A_j, B_{j-1}\}$ genau wie oben unter 3. Wir sehen sogar, daß das Zentrum von $\{A_i, B_j\}$ Elemente des Zentrums von A_i enthält. Schließlich haben wir in der Gruppe $\{A_k, B_k\} = \{A_k, B^*\}$ die gesuchte nilpotente Gruppe, die $\{A_0, B^*\}$ und daher

$$\{a_1 b^{(1)}, a_2 b^{(2)}, \ldots, a_n b^{(n)}\}$$

als Untergruppe enthält. Damit ist Satz 4 bewiesen.

Bemerkung. Wenn die Vermutung zutrifft, daß das Produkt zweier nilpotenter Gruppen auflösbar ist, dann läßt sich Satz 4 in wenigen Zeilen beweisen. Es gilt nämlich nach GRUENBERG [3], daß eine auflösbare, endlich erzeugte Gruppe G nilpotent ist, wenn für je zwei beliebige Elemente x, y von G eine Kommutator-Identität $[x, y, y, \ldots, y] = 1$ besteht.

Beweis von Satz 3. Das Erzeugnis einer beliebigen Menge A_α von lokal-nilpotenten Normalteilern einer Gruppe ist selbst ein lokal-nilpotenter Normalteiler. Denn jedes Element $a \in A$ ist ein endliches Produkt $a_{\alpha_1} a_{\alpha_2} \ldots a_{\alpha_k}$, $a_{\alpha_i} \in A_{\alpha_i}$, also ein Element der Gruppe $\{A_{\alpha_1}, A_{\alpha_2}, \ldots, A_{\alpha_k}\}$, die nach Satz 4 lokal-nilpotent ist. Jedes endliche System $a_1, a_2, \ldots, a_n$ von Elementen von A liegt daher in dem von einer endlichen Menge von A_α's erzeugten Normalteiler; daher ist $\{a_1, \ldots, a_n\}$ nilpotent, was zu beweisen war.

Satz 2 folgt nun in wenigen Schritten, wie beim Beweis von Satz 1.

Beweis von Satz 2. Sei G eine beliebige Gruppe. Jedes Gruppenelement $g \in G$ liegt in einer lokal-nilpotenten, sogar nilpotenten Untergruppe, z.B. der von g erzeugten zyklischen Gruppe. Die Vereinigungsmenge einer beliebigen aufsteigenden Folge von lokal-nilpotenten Untergruppen ist wieder lokal-nilpotent. Daher gibt es nach dem ZORNschen Lemma in jeder beliebigen Gruppe maximale lokal-nilpotente Untergruppen. Sei M eine solche und $N(M)$ ihr Normalisator. Dann ist $N(M)$ sein eigner Normalisator. Denn gäbe es ein Gruppenelement g, das mit $N(M)$ vertauschbar wäre, ohne in $N(M)$ zu liegen, so würde M durch g in eine Gruppe $M' = g^{-1} M g \neq M$ transformiert, die ebenfalls Normalteiler von $N(M)$ und lokal-nilpotent wäre. Dann wäre aber $\{M, M'\}$ nach Satz 4 lokal-nilpotent, im Widerspruch zu der Maximaleigenschaft von M.

Wenn nun G eine Gruppe ist, in der jede echte Untergruppe von ihrem Normalisator verschieden ist, so sehen wir, daß $N(M) = G$, also daß M ein Normalteiler von G ist. Dann umfaßt aber der maximale lokal-nilpotente Normalteiler (Satz 3) alle Elemente von G, d.h., G ist lokal-nilpotent.

Beweis von Satz 5. Sei G eine endlich erzeugte nilpotente Gruppe. Die Kommutator-Faktorgruppe G/G' ist als homomorphes Bild von G ebenfalls endlich erzeugbar. Nach einem Satz von BAER ([1], S. 363), den man auch durch Induktion nach der Klasse von G leicht direkt beweisen kann,

sind dann alle Faktorgruppen G^i/G^{i+1} der unteren Zentralreihe von G endlich erzeugbar, und daher erfüllt G die Maximalbedingung für Untergruppen ([5], Theorem 1.3)[3]).

Ich möchte zum Schluß die Gelegenheit benutzen, einen Irrtum in [9] richtigzustellen, auf den mich G. HIGMAN aufmerksam gemacht hat. Es ist nicht richtig, daß in der von mir dort angegebenen nicht-nilpotenten Gruppe alle maximalen Untergruppen Normalteiler sind. Man kann aber ein Beispiel einer solchen Gruppe herstellen, indem man eine der von HIGMAN und NEUMANN [4] konstruierten nicht-nilpotenten Gruppen ohne maximale Untergruppen mit einer zyklischen Gruppe von Primzahlordnung direkt multipliziert.

Literatur.

[1] BAER, R.: Representations of Groups as Quotient Groups. II. Trans. Amer. Math. Soc. **58**, 348—389 (1945). — [2] FITTING, H.: Beiträge zur Theorie der Gruppen endlicher Ordnung. Jber. dtsch. Math.-Ver. **48**, 77—141 (1938). — [3] GRUENBERG, K.W.: Two Theorems on Engel Groups. Proc. Cambr. Phil. Soc. **49**, 377—380 (1953). — [4] HIGMAN, G., and B. H. NEUMANN: On two Questions of N. Itô. J. London Math. Soc. **29**, 84—88 (1954). — [5] HIRSCH, K. A.: On Infinite Soluble Groups. I. Proc. London Math. Soc. **44**, 53—60 (1938). — [6] HIRSCH, K. A.: On Infinite Soluble Groups. II. Proc. London Math. Soc. **44**, 336—344 (1938). — [7] HIRSCH, K. A.: On Infinite Soluble Groups. III. Proc. London Math. Soc. **49**, 184—194 (1947). — [8] HIRSCH, K. A.: A Characteristic Property of Nilpotent Groups. Proc. Int. Congr. of Math. Cambridge (Mass.) 1950. — [9] HIRSCH, K. A.: Eine kennzeichnende Eigenschaft nilpotenter Gruppen. Math. Nachr. **4**, 47—49 (1951). — [10] KUROŠ, A. G.: Teoriya Grupp, 2. (russische) Aufl. Moskau 1953. — [11] PLOTKIN, B. I.: Zur Theorie der lokal-nilpotenten Gruppen (russisch). Dokl. Akad. Nauk USSR. **76**, 639—641 (1951).

[3]) Andere Beweise von Satz 5 sind kürzlich von P. HALL [Proc. London Math. Soc. (3) **4**, 419—436 (1954)] und von S. A. JENNINGS [Canadian J. of Math. **7**, 169—187 (1955)] veröffentlicht worden [bei der Korrektur hinzugefügt].

Queen Mary College, University of London, London E 1 (England).

(Eingegangen am 4. März 1955.)

Skolem, Th.
Math. Zeitschr. Bd. 63, S. 295—312 (1955)

Einige Bemerkungen über die Auffindung der rationalen Punkte auf gewissen algebraischen Gebilden.

Issai Schur zum Gedächtnis.

Von
Th. Skolem.

Einleitung.

Bekanntlich hat die Frage nach den rationalen Punkten auf einer ebenen algebraischen Kurve eine ziemlich erschöpfende Antwort gefunden in dem Falle einer Kurve vom Geschlecht Null, zum Teil auch für Kurven vom Geschlecht Eins. Meine erste Bemerkung in diesem Aufsatz betrifft die Ausdehnung eines bekannten Satzes über unicursale ebene Kurven auf solche in Räumen beliebiger Dimensionszahl. Ich mache auch eine Bemerkung über Parameterdarstellungen durch gewisse transzendente Funktionen derart, daß die Argumente der rationalen Punkte einen Modul bilden.

Was algebraische Flächen betrifft, so ist es schon schwierig genug, die rationalen zu studieren, d.h. diejenigen, für welche eine Parameterdarstellung mittels rationaler Funktionen möglich ist. Sieht man von den ziemlich trivialen Flächen zweiten Grades ab, so erweist sich bereits das Studium der Flächen dritten Grades im dreidimensionalen Raume als sehr weitläufig. Ihre Behandlung ist oft ziemlich erkünstelt und unsystematisch ausgeführt worden, und meine Bemerkungen im folgenden haben den Zweck, natürlichere Verfahren zu entwickeln.

§ 1.

Ich betrachte Kurven, deren Gleichungen rationale Koeffizienten haben. Ich benutze als eine bekannte geometrische Tatsache, auf deren Beweis ich nicht näher eingehe, daß man das Koordinatensystem so wählen kann, daß die Projektion der betrachteten Kurve in eine der Koordinatenebenen nur endlich viele Punkte besitzt, die gleichzeitig Projektion von mehreren Punkten der Raumkurve sind. Dies bedeutet, daß die Gleichungen der betrachteten Kurve C die Form

$$f(x_1, x_2) = 0, \qquad x_i = g_i(x_1, x_2)/h_i(x_1, x_2), \quad i = 3, \ldots, n$$

haben, wo f und die g_i sowie h_i Polynome mit rationalen Koeffizienten sind. Jeder rationale Punkt von C projiziert sich dann in einen rationalen Punkt der Kurve $f(x_1, x_2) = 0$, welche ich $C_{1,2}$ nenne. Umgekehrt ist jeder rationale Punkt auf $C_{1,2}$ die Projektion eines solchen auf C, wenn eventuell von den

endlich vielen Punkten abgesehen wird, wo für ein i die beiden Polynome g_i und h_i gleichzeitig verschwinden. Durch diese Bemerkung wird klar, daß die Aufgabe, die rationalen Punkte auf einer Raumkurve C zu finden, im wesentlichen auf dieselbe Aufgabe für die Projektionskurve $C_{1,2}$ zurückführbar ist.

Falls nun C unicursal ist, so ist $C_{1,2}$ unicursal, und man kann entscheiden, ob rationale Punkte auf $C_{1,2}$ existieren. Wie üblich nenne ich einen Punkt P gewöhnlich, wenn es darin eine eindeutig bestimmte Tangente gibt, d.h. wenn die Sekante durch zwei benachbarte Punkte P_1 und P_2 eine einzige Grenzstellung besitzt, wenn P_1 und P_2 unabhängig voneinander gegen P streben. Die sonstigen Punkte heißen singulär. Dann hat $C_{1,2}$ entweder keinen gewöhnlichen rationalen Punkt oder unendlich viele, und man kann entscheiden, ob das eine oder das andere eintritt.

Ist nun P ein gewöhnlicher rationaler Punkt auf C, so können wir durch geeignete Wahl des Koordinatensystems erreichen, daß P sich auf $C_{1,2}$ in einen gewöhnlichen rationalen Punkt projiziert. Die unendlich vielen sonst vorhandenen rationalen gewöhnlichen Punkte auf $C_{1,2}$ sind dann die Projektionen von unendlich vielen gewöhnlichen rationalen Punkten auf C. Hierdurch sieht man ein, daß jede unicursale Raumkurve entweder keinen gewöhnlichen rationalen Punkt hat oder deren unendlich viele; außerdem ist entscheidbar, welche Alternative realisiert ist.

Man hat aber bekanntlich auch den Satz (vgl. SKOLEM [7], S. 73):

Eine ebene Kurve vom Geschlecht Null besitzt stets und nur dann einen rationalen gewöhnlichen Punkt, wenn sie mindestens einen gewöhnlichen reellen Punkt enthält und ihre Gleichung in jedem perfekten p-adischen Körper eine Lösung hat, die einen gewöhnlichen Punkt darstellt.

Ich werde eine ganz kurze Überlegung entwickeln, durch die man einsehen kann, *daß dieser Satz auch für jede unicursale Kurve in einem Raume beliebiger Dimensionszahl gültig sein muß.*

Nehmen wir an, daß C einen gewöhnlichen Punkt besitzt in jedem der perfekten p-adischen Körper und im reellen Körper. Es ist bekannt, daß ein gewöhnlicher Punkt in einem solchen Körper nicht isoliert sein kann, so daß in der Tat innerhalb einer gewissen Umgebung von P sogar ein Kontinuum von gewöhnlichen Punkten vorhanden ist. Nennen wir jeden Punkt auf $C_{1,2}$, der entweder singulär ist oder so beschaffen, daß ein g_i gleichzeitig mit h_i verschwindet, einen Ausnahmepunkt, so ist klar, daß entweder P selbst oder ein Nachbarpunkt Q einen Projektionspunkt P' bzw. Q' auf $C_{1,2}$ hat, der kein Ausnahmepunkt ist. Da also $C_{1,2}$ in jedem der perfekten Körper einen gewöhnlichen Punkt hat, so besitzt sie nach dem erwähnten Satz einen rationalen gewöhnlichen Punkt. Wie oben bemerkt, gibt es dann sogar unendlich viele rationale gewöhnliche Punkte auf $C_{1,2}$. Jeder derselben, der kein Ausnahmepunkt ist, gibt zufolge der Gleichungen der Kurve C zu einem rationalen Punkt auf C Anlaß. Hierdurch ist bewiesen, daß der Satz auch für unicursale Raumkurven wahr ist.

§ 2.

Man kann allgemeiner die Lösbarkeit in algebraischen Zahlkörpern untersuchen. Wegen der Zurückführbarkeit auf ebene Kurven, und weil jede ebene Kurve vom Geschlecht Null entweder mit einer Geraden oder einem Kegelschnitt birational mit rationalen Koeffizienten äquivalent ist (nämlich je nachdem der Grad der Kurve ungerade oder gerade ist), so ist diese weitere Lösbarkeitsfrage für unicursale Kurven nur für einen Kegelschnitt aktuell. Man kann wohl kaum sagen, daß man eine wirkliche Übersicht über die kleinsten Körper hat, in denen Lösbarkeit besteht. Es ist aber jedenfalls klar: Wenn Lösbarkeit in einem Körper K stattfindet, der von ungeradem Relativgrad in bezug auf einen Unterkörper k ist, so besteht bereits Lösbarkeit in k. Sei nämlich $2m-1$ der Relativgrad und sei $P, P', \ldots, P^{(2m-2)}$ ein System konjugierter Punkte in bezug auf k. Dann kann man durch diese Punkte eine Kurve m-ten Grades (in der Tat unendlich viele) mit Koeffizienten in k legen; diese schneidet dann den Kegelschnitt in einem einzigen $2m$-ten Punkt Q, dessen Koordinaten dann zu k gehören müssen.

Ein gewisses Gegenstück hierzu ist, daß Körper von beliebig hohem geraden Grade existieren, worin Lösbarkeit nicht stattfindet, sogar Körper, die durch wiederholtes Ausziehen von Quadratwurzeln entstehen. Dies ist sofort klar in dem Falle, wo der Kegelschnitt keinen reellen Punkt besitzt. Sonst ist die Lösbarkeit von

$$a x^2 + b y^2 + c z^2 = 0, \tag{1}$$

wo $(a, b) = (a, c) = (b, c) = 1$ damit gleichbedeutend, daß

$$d = -ab - ac - bc$$

quadratischer Rest modulo abc ist. Nennt man jeden natürlichen Primfaktor p von abc derart, daß $\left(\frac{d}{p}\right) = -1$ ist, einen Nichtteiler, so bleibt Unlösbarkeit in einem Körper K bestehen dann und nur dann, wenn mindestens einer dieser Nichtteiler in K mindestens einen Primidealteiler ungeraden Grades hat. Ist nämlich p ein solches Primideal, g sein Grad, so ist bekanntlich $\left(\frac{d, K}{p}\right)$ gleich $\left(\frac{d}{p}\right)^g$. Betrachtet man z.B. die in rationalen Zahlen $\neq 0$ unlösbare Gleichung

$$x^2 + y^2 - 3 z^2 = 0,$$

so bleibt diese unlösbar in jedem Körper, der durch Adjunktion einer beliebigen Anzahl von Quadratwurzeln $\sqrt{p}$ entsteht, wo $p \equiv 1$ oder $-1 \pmod{12}$. Denn da $\left(\frac{3}{p}\right) = +1$ ist für solche p, so zerlegt sich bekanntlich 3 in jedem dieser Körper in Primideale ersten Grades, so daß -1 quadratischer Nichtrest bleiben muß für diese Primideale. Infolgedessen bleibt die Gleichung auch unlösbar in dem Körper unendlich hohen Grades, der von sämtlichen Quadratwurzeln $\sqrt{p}$ mit $p \equiv \pm 1 \pmod{12}$ herrührt.

Was insbesondere die Lösbarkeit von (1) im quadratischen Körper $k(\sqrt{m})$ betrifft, so findet man leicht, daß sie mit der Lösbarkeit der quaternären Gleichung

$$a x^2 + b y^2 + c z^2 + m a b c u^2 = 0$$

in rationalen Zahlen gleichwertig ist. Hieraus folgt wieder unter anderem, daß $a x^2 + b y^2 + c z^2$ eine universale Form ist, d.h. jede rationale Zahl darstellt für gewisse rationale Werte von x, y, z, wenn sie eine Nullform ist, d.h. (1) rational lösbar ist. Wegen einer ähnlichen Betrachtung im folgenden ist es zweckmäßig, hier zu bemerken: *Wenn* (1) *lösbar ist, so ist die Gleichung*

$$a x^2 + b y^2 + c z^2 = r \tag{2}$$

durch lineare Ausdrücke

$$x = a_1 r + a_2, \quad y = b_1 r + b_2, \quad z = c_1 r + c_2 \tag{3}$$

identisch in r lösbar. Sind in der Tat (a_1, b_1, c_1) und (a_2', b_2', c_2') zwei verschiedene rationale Punkte auf dem Kegelschnitt (1), so ist

$$a a_1 a_2' + b b_1 b_2' + c c_1 c_2' \neq 0,$$

und folglich kann man a_2, b_2, c_2 proportional a_2', b_2', c_2' so wählen, daß (2) mittels (3) erfüllt wird. Man kann aber auch weitere Parameterlösungen in unübersehbarer Menge herleiten. Immer, wenn (a_3, b_3, c_3) ein rationaler Punkt P auf (1) ist, dagegen (a_4, b_4, c_4) ein Punkt auf der Tangente in P, dann ergibt

$$x = a_3 s + a_4, \quad y = b_3 s + b_4, \quad z = c_3 s + c_4$$

eine Lösung von

$$a x^2 + b y^2 + c z^2 = h,$$

wo h eine gewisse rationale Konstante ist. Bedeuten i, j Quaternionen derart, daß

$$i^2 = -ab, \quad j^2 = -ac, \quad ij + ji = 0,$$

und bildet man das Produkt

$$\begin{aligned}(a(a_3 s + a_4) + (b_3 s + b_4) i + (c_3 s + c_4) j)\,(a(a_1 r + a_2) + (b_1 r + b_2) i + \\ + (c_1 r + c_2) j)\,(a(a_3 s + a_4) + (b_3 s + b_4) i + (c_3 s + c_4) j) \\ = aA + Bi + Cj,\end{aligned}$$

wo A, B, C Polynome sind, die quadratisch in bezug auf s und linear in r sind, so erkennt man, daß

$$a A^2 + b B^2 + c C^2 = a^2 h^2 r$$

identisch in s und r erfüllt ist. — Mittels derselben Methode kann man weitere Lösungen der Gl. (2) erhalten, wo x, y, z als Polynome in $r, s_1, s_2, \ldots$ ausgedrückt sind, so daß (2) identisch in allen Variablen erfüllt ist.

Bekanntlich hat man den MORDELL-WEILschen Satz, daß die rationalen Punkte auf Kurven vom Geschlecht 1 mittels elliptischer Funktionen eines Parameters gegeben sind, wobei die Argumente einen Modul bilden. Man

muß erwarten, daß etwas Analoges für die einfacheren Kurven vom Geschlecht Null stattfindet. Dies ist nun insofern in trivialer Weise der Fall, als man ja die rationalen Werte eines Parameters x durch die Gleichung $x = e^u$ ausdrücken kann, und dann bilden die zugehörigen Argumentwerte von u einen Modul. Der Unterschied ist offenbar nur, daß man für die unicursalen Kurven einen Modul mit unendlicher Basis hat; man kann also, wenn man den Begriff des Ranges für diese Kurven benutzen will, sagen, daß sie einen unendlichen Rang haben. Von etwas größerem Interesse ist aber die folgende Parameterdarstellung der Lösungen der Gleichung

$$x^2 - m y^2 = 1 . \tag{4}$$

Die allgemeine Lösung ist hier durch den Ansatz

$$x + y\sqrt{m} = \frac{u + v\sqrt{m}}{u - v\sqrt{m}}$$

gegeben, wo u und v ganze Zahlen sind, nicht beide Null. Nach einem Satze, den ich vor einigen Jahren bewiesen habe [8] besitzt die multiplikative Gruppe aller Zahlen $\neq 0$ eines algebraischen Körpers stets eine, allerdings unendliche, Basis. Dies ist trivial, wenn die Anzahl der Idealklassen 1 ist, ist aber auch sonst wahr. Man hat deshalb

$$u + v\sqrt{m} = \pi_1^{x_1} \pi_2^{x_2} \dots ,$$

wo die π_r Basiselemente sind. Hieraus folgt

$$x + y\sqrt{m} = \alpha_1^{x_1} \alpha_2^{x_2} \dots , \tag{5}$$

wobei $\alpha_r = \frac{\pi_r}{\pi_r'}$. Ich illustriere die Anwendung dieser Formel (5) an einigen typischen Beispielen.

Beispiel 1. Sämtliche rationalen Punkte auf dem Kreise

$$x^2 + y^2 = 1$$

sind gegeben durch die Formeln

$$x = \cos(\alpha_1 x_1 + \alpha_2 x_2 + \cdots), \quad y = \sin(\alpha_1 x_1 + \alpha_2 x_2 + \cdots) .$$

Dabei sind die x_r beliebige ganze rationale Zahlen; die Zahlen α_r sind dadurch bestimmt, daß

$$\cos\alpha_r + i \sin\alpha_r = \frac{\pi_r^2}{p_r}$$

ist, wo π_r die Faktoren $a + bi$ mit $a > 0$, $b > 0$ aller natürlicher Primzahlen p_r der Form $4h+1$ und der Zahl 2 durchläuft.

Beispiel 2. Sämtliche rationalen Punkte auf der Kurve

$$x^2 + 5 y^2 = 1$$

sind gegeben durch

$$x = \cos(\alpha_1 x_1 + \alpha_2 x_2 + \cdots), \quad y = \frac{1}{\sqrt{5}} \sin(\alpha_1 x_1 + \alpha_2 x_2 + \cdots),$$

wenn jetzt die α_r erstens die Zahlen $\frac{\pi_r^2}{p_r}$ durchlaufen, wo π_r den Faktor $a + b\sqrt{-5}$ mit $a > 0$, $b > 0$ der natürlichen Primzahlen $\equiv 1,9 \pmod{20}$ bedeutet, und wenn die α_r zweitens alle Zahlen durchlaufen, wo π_r den Faktor derselben Art der Zahlen $2p$ bedeutet, p eine natürliche Primzahl $\equiv 3,7 \pmod{20}$. Denn -1, 2, die natürlichen Primzahlen $\equiv 11, 13, 17, 19 \pmod{20}$, die Zahlen $a + b\sqrt{-5}$, $a > 0$, $b \neq 0$, welche Faktoren der Primzahlen $\equiv 1,9 \pmod{20}$ sind, bilden zusammen mit den Zahlen $a + b\sqrt{-5}$, $a > 0$, $b \neq 0$, welche Faktoren von $2p$ mit $p \equiv 3,7 \pmod{20}$ sind, eine Basis der multiplikativen Gruppe aller Zahlen $\neq 0$ des Körpers $k(\sqrt{-5})$.

Beispiel 3. Für $m = 2$ sind die rationalen Lösungen von (4) gegeben durch

$$x = \cosh(\alpha_1 x_1 + \alpha_2 x_2 + \cdots), \quad y = \frac{1}{\sqrt{2}} \sinh(\alpha_1 x_1 + \alpha_2 x_2 + \cdots),$$

wobei etwa

$$\cosh \alpha_1 = -1, \quad \sinh \alpha_1 = 0; \quad \cosh \alpha_2 = 3, \quad \sinh \alpha_2 = 2\sqrt{2},$$

während die folgenden α_r der Reihe nach so bestimmt sind, daß

$$\cosh \alpha_r + \sinh \alpha_r = \frac{\pi_r^2}{p_r}, \quad p_r = \operatorname{Norm} \pi_r = \pi_r \pi_r', \quad p_r \equiv \pm 1 \pmod{8}.$$

Für $m > 0$ ist auch die Gleichung

$$x^2 - m y^2 = -1$$

rational lösbar, wenn -1 quadratischer Rest mod m ist. Diese Lösungen können in derselben Form

$$x = \cosh A, \quad y = \frac{1}{\sqrt{m}} \sinh A$$

dargestellt werden; hierin durchläuft aber jetzt A die Elemente eines Nebenmoduls, nämlich $A = \frac{\pi}{2} i + B$, wo B die Elemente des Moduls durchläuft derart, daß

$$x = \cosh B, \quad y = \frac{1}{\sqrt{m}} \sinh B$$

die rationalen Lösungen von (4) liefern. Übrigens kann man auch sagen, daß

$$x = \sinh B, \quad y = \frac{1}{\sqrt{m}} \cosh B,$$

die Lösungen von $x^2 - m y^2 = -1$ darstellen.

Für die allgemeinere Gleichung

$$a x^2 + b y^2 = c \tag{6}$$

können die rationalen Lösungen dargestellt werden mittels Argumentwerten aus einem Nebenmodul. Ist nämlich x_0, y_0 eine spezielle Lösung, so sind die anderen gegeben mittels der Gleichung

$$x\sqrt{a} + y\sqrt{-b} = (x_0\sqrt{a} + y_0\sqrt{-b})(u + \sqrt{-ab}\,v),$$

wo

$$u^2 + ab\,v^2 = 1. \tag{7}$$

Man findet hieraus als allgemeine Lösung von (6) im Falle $ab > 0$

$$x = \sqrt{\frac{c}{a}}\cos(\alpha - A), \quad y = \sqrt{\frac{c}{b}}\sin(\alpha - A);$$

dabei ist α so zu bestimmen, daß

$$x_0 = \sqrt{\frac{c}{a}}\cos\alpha, \quad y_0 = \sqrt{\frac{c}{b}}\sin\alpha$$

ist, während A alle Zahlen eines Moduls durchläuft, so daß

$$u = \cos A, \quad v = \frac{1}{\sqrt{ab}}\sin A$$

alle Lösungen von (7) liefern. Für $ab < 0$ hat man ähnliche Gleichungen mit cosh und sinh anstatt cos und sin.

Ich möchte noch ein Beispiel erwähnen, nämlich eine Parameterdarstellung der rationalen Punkte auf der unicursalen kubischen Kurve, deren Gleichung in der Form

$$y^2 = x^2(x + a)$$

angenommen wird. Ist $a < 0$, so hat man mit α als Parameter

$$x = -a/\sin^2\alpha, \quad y = -a\sqrt{-a}\cos\alpha/\sin^3\alpha.$$

Man erkennt, daß $\cos 2\alpha$ und $\sqrt{-a}\sin 2\alpha$ rational werden, und daß also für die rationalen Punkte α einen Modul durchläuft, der aus den Hälften der Zahlen besteht, welche die Werte des Parameters ausmachen, die nach der obigen Ausführung die Lösungen der Gleichung

$$x^2 - 1/a\,y^2 = 1$$

liefern. Ist $a > 0$, bekommt man in analoger Weise

$$x = a/\sinh^2\alpha, \quad y = (a\sqrt{a}/\sinh^3\alpha)\cdot\cosh\alpha$$

für die Zweige der Kurve zwischen dem Doppelpunkt und ∞ und für das Oval

$$x = a/\cosh^2\alpha, \quad y = a\sqrt{a}\sinh\alpha/\cos h^3\alpha,$$

und man findet wieder, daß die rationalen Punkte durch die Werte von α in einem Modul gegeben sind.

§ 3.

In diesem Paragraphen werde ich die rationalen Punkte auf kubischen Flächen betrachten, die singuläre Punkte enthalten, aber keine Regelflächen sind (vgl. SEGRE [4]; [5]). Bekanntlich können höchstens vier Doppelpunkte vorkommen. Da ich natürlich voraussetze, daß die Gleichung der Fläche rationale Koeffizienten hat, so muß, falls nur ein Doppelpunkt vorkommt, dieser rational sein, falls zwei vorkommen, müssen sie entweder beide rational sein, oder sie sind konjugiert quadratisch irrational, usw. Infolgedessen ist es klar, daß es genügt, die folgenden vier Fälle zu behandeln:

1. Ein rationaler Doppelpunkt.
2. Zwei konjugiert quadratisch irrationale Doppelpunkte.
3. Drei konjugiert kubisch irrationale Doppelpunkte.
4. Vier konjugiert biquadratisch irrationale Doppelpunkte.

Nach dem Grade der Schwierigkeit werde ich diese Fälle in der Reihenfolge 1., 4., 3., 2. behandeln.

1. Ist P der rationale Doppelpunkt, so schneidet jede rationale Gerade durch P die Fläche in einen rationalen Punkt Q, und ist umgekehrt Q ein beliebiger rationaler Punkt der Fläche, so ist die Verbindungslinie zwischen P und Q rational. Man bekommt hierdurch in trivialer Weise die Koordinaten der rationalen Punkte rational ausgedrückt durch die Winkelkoeffizienten k und l der Geraden durch P.

Ein Sonderfall hiervon ist, daß eine der Unbekannten der homogen angenommenen Gleichung, etwa u, nur linear auftritt; dann kann man u als (gebrochene) rationale Funktion von x, y, z ausdrücken.

4. Die vier konjugierten Doppelpunkte seien P_i mit Koordinaten $x^{(i)}$, $y^{(i)}$, $z^{(i)}$, $u^{(i)}$, und es sei $\xi_j = 0$ die Ebene, welche alle P_i außer P_j enthält. Dann ist z.B. ξ_1 die Determinante

$$\begin{vmatrix} x^{(2)} & y^{(2)} & z^{(2)} & u^{(2)} \\ x^{(3)} & y^{(3)} & z^{(3)} & u^{(3)} \\ x^{(4)} & y^{(4)} & z^{(4)} & u^{(4)} \\ x & y & z & u \end{vmatrix},$$

also mit konjugierten $\alpha^{(j)}(\beta^{(j)}, \gamma^{(j)}, \delta^{(j)})$

$$\xi_j = \alpha^{(j)} x + \beta^{(j)} y + \gamma^{(j)} z + \delta^{(j)} u.$$

Man sieht, daß dann umgekehrt x, y, z, u durch $\xi_1, \xi_2, \xi_3, \xi_4$ so ausgedrückt sind:

$$(8) \quad \begin{cases} x = \alpha_1 \xi_1 + \alpha_2 \xi_2 + \alpha_3 \xi_3 + \alpha_4 \xi_4, & y = \beta_1 \xi_1 + \beta_2 \xi_2 + \beta_3 \xi_3 + \beta_4 \xi_4, \\ z = \gamma_1 \xi_1 + \gamma_2 \xi_2 + \gamma_3 \xi_3 + \gamma_4 \xi_4, & u = \delta_1 \xi_1 + \delta_2 \xi_2 + \delta_3 \xi_3 + \delta_4 \xi_4, \end{cases}$$

wo die α (und ebenso β, γ, δ) für sich konjugiert in den betreffenden biquadratischen Körpern sind. Durch Einsetzen von $\xi_1, \xi_2, \xi_3, \xi_4$ statt x, y, z, u muß die Gleichung der Fläche bekanntlich die Form annehmen

$$\varepsilon_1 \xi_2 \xi_3 \xi_4 + \varepsilon_2 \xi_1 \xi_3 \xi_4 + \varepsilon_3 \xi_1 \xi_2 \xi_4 + \varepsilon_4 \xi_1 \xi_2 \xi_3 = 0,$$

und dabei müssen augenscheinlich hier $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ konjugiert werden. Diese Gleichung kann einfacher

$$S \frac{\varepsilon_1}{\xi_1} = 0$$

geschrieben werden, wo S die Spur bedeutet. Mittels dreier rationaler Parameter kann man nun die allgemeine Lösung der Gleichung

$$S \tau_1 = 0$$

angeben, und dann liefert

$$\xi_1 = \frac{\varepsilon_1}{\tau_1}$$

den allgemeinen Ausdruck für ξ_1. Mittels (8) findet man hieraus

$$x = S \frac{\alpha_1 \varepsilon_1}{\tau_1}, \quad y = S \frac{\beta_1 \varepsilon_1}{\tau_1}, \quad z = S \frac{\gamma_1 \varepsilon_1}{\tau_1}, \quad u = S \frac{\delta_1 \varepsilon_1}{\tau_1}$$

als eine vollständige Parameterdarstellung der rationalen Lösungen.

3. Mittels linearer Transformation mit rationalen Koeffizienten kann die Gleichung der Fläche auf eine solche Form gebracht werden, daß die drei Doppelpunkte P_1, P_2, P_3 in der Ebene $x = 0$ liegen. Es seien K_1, K_2, K_3 die konjugierten kubischen Körper, wozu die Koordinaten von P_1, P_2, P_3 gehören. Weiter sei $\xi_1 = 0$ eine Ebene, welche P_2, P_3 enthält; es ist klar, daß ξ_1 so wählbar ist, daß ihre Koeffizienten zu K_1 gehören. Unter ξ_2 und ξ_3 verstehe ich die konjugierten Linearformen mit Koeffizienten aus K_2 und K_3. Die Gleichung der Fläche wird dann

$$a x^3 + \beta_1 x^2 \xi_1 + \beta_2 x^2 \xi_2 + \beta_3 x^2 \xi_3 + x(\gamma_1 \xi_2 \xi_3 + \gamma_2 \xi_1 \xi_3 + \gamma_3 \xi_1 \xi_2) + \\ + d \xi_1 \xi_2 \xi_3 = 0,$$

wobei β_i und γ_i für $i = 1, 2, 3$ konjugierte Zahlen aus K_1, K_2, K_3 sind, a und d rational. Setzt man nun

$$\xi_i + \frac{\gamma_i}{d} x = \bar{\xi}_i,$$

so geht die Gleichung über in

$$\bar{a} x^3 + (\bar{\beta}_1 \bar{\xi}_1 + \bar{\beta}_2 \bar{\xi}_2 + \bar{\beta}_3 \bar{\xi}_3) x^2 + d \bar{\xi}_1 \bar{\xi}_2 \bar{\xi}_3 = 0,$$

wobei hier

$$\bar{a} = a - S \frac{\beta_1 \gamma_1}{d} + \frac{2 N \gamma_1}{d^2}, \quad \bar{\beta}_1 = \beta_1 - \frac{\gamma_2 \gamma_3}{d}, \ldots$$

gesetzt ist. Sind die $\bar{\beta}_r$ alle $= 0$, hat man eine Gleichung, deren allgemeine Lösung sofort angebbar ist. Ich sehe deshalb davon ab. Setzt man nun

$$\frac{\bar{\beta}_i \bar{\xi}_i}{x} = \eta_i, \quad \bar{d} = \frac{d}{\bar{\beta}_1 \bar{\beta}_2 \bar{\beta}_3},$$

so nimmt unsere Gleichung die Gestalt

$$\bar{a} + S \eta + \bar{d} N \eta = 0$$

an. Ich werde nun die Gleichung

$$N\tau + hS\tau + k = 0 \tag{9}$$

zuerst in dem Sonderfall behandeln, wo die drei konjugierten Körper K_1, K_2, K_3, welche von den Wurzeln τ herrühren, rein-kubisch sind. Danach werde ich bei beliebig gelassenem Körper K_1 den Fall betrachten, wo die Wurzeln der Gleichung

$$t^3 + 3ht + k = 0 \tag{10}$$

zu rein kubischen Körpern Anlaß geben. Zuletzt betrachte ich den allgemeinen Fall. Ich werde zeigen, wie man mindestens in den beiden zuerst erwähnten Fällen eine vollständige Parameterdarstellung der rationalen Lösungen angeben kann, sofern solche überhaupt existieren.

Es sei K_1 der Körper $k(\vartheta)$, $\vartheta^3 = m$. Soll (9) von einer Zahl $\tau \in k(\vartheta)$ erfüllt sein, so kann man τ in der Form

$$\tau = \frac{a + b\vartheta}{c + d\vartheta}$$

schreiben, und man bekommt

$$N(a + b\vartheta) + hS(a + b\vartheta)(c + \varrho\, d\vartheta)(c + \varrho^2 d\vartheta) + kN(c + d\vartheta) = 0$$

oder

$$a^3 + mb^3 + 3h(ac^2 + mbd^2) + k(c^3 + md^3) = 0,$$

d.h.

$$a^3 + 3hac^2 + kc^3 + m(b^3 + 3hbd^2 + kd^3) = 0. \tag{11}$$

Dies bedeutet, daß m die Norm einer Zahl des Körpers ist, der von einer Wurzel α der Gl. (10) herrührt. In der Tat bedeutet (11) dasselbe wie

$$-m = N\frac{a - c\alpha}{b - d\alpha}. \tag{12}$$

Die Gl. (9) ist also stets und nur dann lösbar, wenn (12) es ist, und das kann bekanntlich immer entschieden werden. (Näheres über die Lösbarkeit weiter unten.) Die allgemeine Lösung von

$$N\Theta = -m$$

im Körper $k(\alpha)$ ist gegeben durch

$$\Theta = \Theta_0 \Phi,$$

wo Θ_0 eine spezielle Lösung ist, während Φ die allgemeine Lösung von

$$N\Phi = 1$$

ist; diese nehme ich als bekannt an. Setzt man dann

$$\Theta = \frac{a - c\alpha}{b - d\alpha} = t_0 + t_1\alpha + t_2\alpha^2,$$

so bekommt man

$$t_2 b - t_1 d = 0, \quad a = t_0 b + k t_2 d, \quad c = t_0 d - t_1 b - 3h t_2 d,$$

d.h.

$$b = \frac{t_1}{t_2} d, \quad a = \left(\frac{t_0 t_1}{t_2} + k t_2\right) d, \quad c = \left(t_0 - \frac{t_1^2}{t_2} - 3 h t_2\right) d.$$

Folglich ist

$$\tau = \frac{t_0 t_1 + k t_2^2 + t_1 \vartheta}{t_0 t_2 - t_1^2 - 3 h t_2^2 + t_2 \vartheta}$$

die allgemeine Lösung von (9).

Danach betrachte ich den Fall, daß der Körper $k(\alpha) = k(\vartheta)$ ist, $\vartheta^3 = m$, m rational. Dann müssen rationale Zahlen a, b, c, d derart existieren, daß

$$\vartheta = \frac{a\alpha + b}{c\alpha + d}$$

und folglich

$$(a\alpha + b)^3 + m(c\alpha + d)^3 = 0$$

ist, woraus

$$a^3 + m c^3 : a^2 b + m c^2 d : a b^2 + m c d^2 : b^3 + m d^3 = 1 : 0 : h : k$$

folgt. Wegen

$$N(a\tau + b) = a^3 N\tau + a^2 b S\tau\tau' + a b^2 S\tau + b^3$$
$$m N(c\tau + d) = m(c^3 N\tau + c^2 d S\tau\tau' + c d^2 S\tau + d^3)$$

erkennt man dann, daß (9) in der Form

$$N\Theta_1 + m N\Theta_2 = 0$$

mit

$$\Theta_1 = a\tau + b, \quad \Theta_2 = c\tau + d$$

geschrieben werden kann. Ist also Θ die allgemeine Lösung von

$$N\Theta = -m,$$

so ist

$$\tau = \frac{b - d\Theta}{a - c\Theta}$$

die allgemeine Lösung von (9).

Im allgemeinen Falle kann man folgendermaßen vorgehen. Es sei $K_1 = k(\vartheta_1)$, ϑ_1 eine Wurzel der Gleichung

$$\vartheta^3 + c_1\vartheta^2 + c_2\vartheta + c_3 = 0, \tag{13}$$

deren Diskriminante D heißen möge. Dann ist der Körper $K_1(\sqrt{-3D}) = k(\vartheta_1, \sqrt{-3D})$ rein kubisch in bezug auf $k(\sqrt{-3D})$. Man kann deshalb in derselben Weise wie oben die allgemeine Lösung von (9) mit Koordinaten im Körper $k(\sqrt{-3D})$ finden, also die allgemeine Lösung von (9) mit τ in $K_1(\sqrt{-3D})$. Zieht man nun eine Sekante durch ein beliebiges Paar von Punkten P_1 und P_2, deren Koordinaten konjugierte Zahlen in $k(\sqrt{-3D})$ sind, so wird der dritte Schnittpunkt mit der Fläche ein rationaler Punkt P. Ob man aber in dieser Weise wirklich die allgemeine Lösung in rationalen Zahlen findet, muß hier offen gelassen werden. Ich habe leider keine Zeit gehabt, auf diese Frage ernstlich einzugehen.

SEGRE [5] gibt an, wie man eine vollständige Parameterdarstellung der rationalen Punkte erhalten kann, wenn man zuerst zwei rationale Punkte P und Q gefunden hat. Sind O_1, O_2, O_3 die drei singulären Punkte, so sieht man leicht ein, daß von den fünf Punkten O_1, O_2, O_3, P, Q nie vier in einer Ebene liegen. Jede windschiefe kubische Kurve durch O_1, O_2, O_3, P, Q mit rationalen Koeffizienten schneidet dann die kubische Fläche in einen einzigen weiteren, also rationalen, Punkt. Umgekehrt geht durch jeden rationalen Punkt der Fläche eine solche kubische Kurve.

2. Mittels linearer Transformation mit rationalen Koeffizienten kann man erreichen, daß die Doppelpunkte die Koordinaten $0, 0, \sqrt{m}$ und $0, 0, -\sqrt{m}$ bekommen, m rational. Die ganze z-Achse liegt dann in der Fläche. Legt man eine Ebene $y = kx$ durch die z-Achse, k rational, so schneidet diese die kubische Fläche in einen Kegelschnitt. In bekannter Weise kann man dann für jeden Wert von k entscheiden, ob rationale Punkte auf dem Kegelschnitt existieren, und auch eine allgemeine Formel für diese aufstellen. Man bekommt jedoch hierdurch nicht eine Parameterdarstellung der rationalen Lösungen überhaupt, weil man gewöhnlich nicht eine solche Darstellung für die Werte derjenigen k hat, für welche Lösbarkeit besteht. Es ist aber klar, daß man genau wie im Fall 1 hier eine vollständige Parameterdarstellung der Lösungen im Körper $k(\sqrt{m})$ aufstellen kann. Zieht man dann die Sekante zwischen zwei beliebigen konjugierten Punkten, so wird der dritte Schnittpunkt rational. Allerdings bleibt es hier wiederum fraglich, ob man alle rationalen Punkte auf der Fläche in dieser Weise erhält.

Gibt es einen dritten oder sogar einen vierten Doppelpunkt, so kann man leicht eine vollständige Parameterdarstellung erhalten. Gibt es genau drei Doppelpunkte, so ist ja der dritte rational, und man gelangt zum Fall 1 zurück. Gibt es zwei weitere Doppelpunkte, so sind diese entweder rational, so daß man wieder den Fall 1 hat, oder sie sind auch konjugiert quadratisch irrational. In dem letzten Fall kann man aber so vorgehen wie im Fall 4.

Es geht aus dem obigen hervor, daß in den Fällen 1, 2, 4 stets rationale Punkte auf der Fläche vorkommen. Im Fall 3 ist es aber nicht immer so. MORDELL ([3], S. 6) hat die Vermutung aufgestellt, daß die Gleichung $f(x, y, z, u) = 0$, wo f eine kubische Form ist, dann — und selbstverständlich auch nur dann — eine rationale Lösung hat, wenn die Kongruenz $f(x, y, z, u) \equiv 0$ für jeden Modul lösbar ist. *Ich werde hier zeigen, daß diese Vermutung richtig ist im Fall 3 und also überhaupt für kubische Flächen, die mindestens einen singulären Punkt besitzen.* (E. S. SELMER [6] hat die Richtigkeit der Vermutung für die Flächen $a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 + a_4 x_4^3 = 0$ unter der Voraussetzung bewiesen, daß $a_3 a_4 / a_1 a_2$ ein rationaler Kubus ist.)

Ich stütze den Beweis auf die folgende bekannte Tatsache. Ist K ein zyklischer kubischer Oberkörper über dem Körper k und ist $m \in k$, so besitzt die Gleichung

$$N\tau = m \tag{14}$$

eine Lösung $\tau \in K$, wenn die entsprechende Kongruenz

$$N\tau \equiv m \tag{15}$$

für jeden Modul lösbar ist (vgl. HASSE [2], S. 40). Es sei jetzt K ein nichtzyklischer kubischer Oberkörper über k. Dann ist die normale Erweiterung $\overline{K}$ vom sechsten Grade über k zyklisch über einen relativ quadratischen Oberkörper k_2 über k. Ist nun (15) lösbar für jeden Modul im Körper k, so ist dies um so mehr der Fall im Körper k_2. Nach dem zitierten Satz muß dann (14) in $\overline{K}$ lösbar sein. Dies bedeutet, daß die kubische Gleichung für die Koeffizienten von τ, wenn τ als Linearform mittels einer Basis in k ausgedrückt ist, in Zahlen aus k_2 lösbar ist. Die Anwendung der Sekantenmethode zeigt dann, daß sie auch in k lösbar sein muß. Aus dieser Verallgemeinerung folgert man leicht die Gültigkeit der MORDELLschen Vermutung in den zwei Sonderfällen von 3, die oben erwähnt sind. Im allgemeinen Falle kann man so schließen: Es sei wie früher D die Diskriminante von (13). Es werde angenommen, daß die Kongruenz

$$N\tau + h S\tau + k \equiv 0 \tag{16}$$

im absolut rationalen Zahlkörper für jeden Modul lösbar ist. Dann ist sie um so mehr lösbar in $k(\sqrt{-3D})$ für jeden Modul. Im Körper $k(\sqrt{-3D})$ ist aber (9) mit (12) gleichwertig, wo jetzt m durch eine Zahl μ in $k(\sqrt{-3D})$ ersetzt ist. Die Kongruenz (16) ist mit einer entsprechenden Kongruenz

$$N\Theta_1 + \mu N\Theta_2 = 0$$

gleichwertig. Da also diese für jeden Modul lösbar ist, so ist (12) lösbar in $k(\sqrt{-3D})$, woraus folgt, daß (9) in demselben Körper lösbar ist. Mittels der Sekantenmethode sieht man dann ein, daß (9) auch rational lösbar ist.

§ 4.

Ich werde nun die allgemeinen kubischen Flächen betrachten, aber mit Ausschluß der Regelflächen.

Es verdient bemerkt zu werden, daß die Unterscheidung zwischen den Flächen ohne singuläre Punkte und den Flächen mit solchen für das Problem der rationalen Punkte nicht immer wesentlich ist. *In der Tat kommt es oft vor, daß eine birationale Transformation mit rationalen Koeffizienten existiert, die eine Fläche ohne singuläre Punkte in eine mit solchen überführt.* Ich gebe ein Beispiel.

Die kubische Fläche

$$x^3 + 2y^3 + 3z^3 + 6u^3 = 0 \tag{17}$$

besitzt keinen singulären Punkt. Aber durch die Transformation

$$x : y : z : u = -t_0 t_1 + 2t_2^2 : -t_1^2 + t_0 t_2 : -t_1 t_3 : t_2 t_3$$

geht sie über in

$$t_0^3 + 2t_1^3 + 4t_2^3 - 6t_0 t_1 t_2 + 3t_3^3 = 0, \tag{18}$$

und diese Fläche hat die drei Doppelpunkte

$$t_0 : t_1 : t_2 : t_3 = \begin{cases} \vartheta^2 : \vartheta : 1 : 0 \\ \varrho^2 \vartheta^2 : \varrho \vartheta : 1 : 0 \\ \varrho \vartheta^2 : \varrho^2 \vartheta : 1 : 0 \end{cases}$$

mit $\vartheta^3 = 2$, $\varrho^2 + \varrho + 1 = 0$. Die umgekehrte Transformation ist

$$t_0 : t_1 : t_2 : t_3 = x z^2 + 2 y u^2 : y z^2 - x z u : x u^2 - y z u : z^3 + 2 u^3.$$

Da die allgemeine Lösung von (18) leicht angebbar ist, so findet man hierdurch leicht die allgemeine Lösung von (17).

Man könnte fragen, ob nicht vielleicht jede kubische Fläche birational in eine solche mit singulären Punkten transformierbar ist. Wie nun dies sein mag, so wird es wohl ein Problem sein, die betreffenden Transformationen zu finden; deshalb dürfte es wohl auf alle Fälle berechtigt sein, die Flächen zu studieren, die keinen Doppelpunkt besitzen.

Bekanntlich kann man in dem Falle, wo die Fläche zwei rationale Geraden l_1 und l_2 enthält, die nicht in derselben Ebene liegen, in trivialer Weise eine vollständige Parameterdarstellung ihrer rationalen Punkte aufstellen. In der Tat, eine Gerade, die einen rationalen Punkt auf l_1 mit einem solchen auf l_2 verbindet, schneidet die Fläche in einen dritten rationalen Punkt. Ist umgekehrt P ein rationaler Punkt der Fläche, so liegt P zugleich mit l_1 in einer rationalen Ebene, welche l_2 in einen rationalen Punkt P_2 schneidet. Die Gerade welche P_2 mit P verbindet, schneidet dann l_1 in einen rationalen Punkt P_1.

Abgesehen von diesem Falle aber scheint es meistens schwierig, eine vollständige Darstellung der rationalen Punkte zu geben. Man hat sich dann damit begnügt, Scharen von Lösungen mit einem oder mehreren Parametern zu finden, ohne auf die Frage einzugehen, ob sie alle Lösungen enthalten. In erster Instanz hat man nun beweisen können, daß, falls ein rationaler Punkt auf der Fläche vorkommt, unendlich viele solche vorhanden sind. Für diesen Satz haben SEGRE und R. F. WHITEHEAD Beweise gegeben. Der Beweis WHITEHEADs wird l. c. von MORDELL wiedergegeben mit der Bemerkung, daß er so elementar ist, daß es überraschend ist, daß er nicht früher entdeckt worden ist, z. B. von EULER. Es ist richtig, daß der Beweis elementar ist, aber er beruht doch auf einem Kunstgriff. Ich möchte deshalb einen anderen Beweis vorschlagen, der mir natürlicher zu sein scheint.

Bekanntlich wird die Tangentenebene T in einem Punkt P gewöhnlich die Fläche in einer Kurve C dritten Grades mit Doppelpunkt in P schneiden. Ist P rational, so ist T eine rationale Ebene, und jede rationale Gerade durch P in T schneidet dann C in einen rationalen Punkt. Dies gibt sofort eine einparametrige Schar von rationalen Punkten. Nun kann es sein, daß C zerfällt in eine Gerade und einen Kegelschnitt durch P; diese sind dann rational, so daß wir wiederum unendlich viele rationale Punkte erhalten. Es kann aber auch eintreten, daß C sich zerlegt in drei Geraden. Ist mindestens eine dieser Geraden rational, so gibt es wieder unendlich viele rationale

Punkte. Es bleibt deshalb nur der Fall, daß T die Fläche in drei Geraden l_1, l_2, l_3 schneidet, welche konjugiert kubisch irrational sind. Ferner müssen l_1, l_2, l_3 alle durch P gehen; denn sonst wären die drei Schnittpunkte dieser Geraden alle rational, da sie konjugiert sind, und dann wären alle drei Geraden rational. Es kann dann auch sofort bemerkt werden, daß jede sonstige Ebene durch P die Fläche in einer Kurve schneiden muß, die in P einen Wendepunkt hat. Ich nenne einen Punkt P einen Ausnahmepunkt, wenn die zugehörige Tangentenebene T die Fläche in drei Geraden l_1, l_2, l_3 schneidet, die konjugiert in kubischen Körpern sind. Es ist klar, daß nur endlich viele Ausnahmepunkte existieren können; denn es gibt ja auf der Fläche höchstens 27 Geraden.

Es sei also P ein rationaler Ausnahmepunkt. Ich lege eine rationale Gerade l durch P. Diese schneidet die kubische Fläche in zwei Punkten P_1 und P_2, deren Koordinaten konjugiert in einem quadratischen Körper K sind. Die Gerade l kann natürlich so gewählt werden, daß weder P_1 nach P_2 einer der endlich vielen Ausnahmepunkte wird. Sollten P_1 und P_2 beide rational ausfallen, so bewirkt das nur, daß in der folgenden Überlegung K einen beliebigen quadratischen Körper bedeuten kann. Wir nehmen dann eine Ebene E_1 durch l mit Koeffizienten aus K, jedoch nicht alle rational. Dann schneidet E_1 die zu P_1 gehörige Tangentialebene T_1 in einer Geraden l_1, welche die Fläche in einem Punkt Q_1 mit Koordinaten in K schneidet. Die Ebene E_2 durch l hat dann Koeffizienten in K, konjugiert zu denen der Ebene E_1; und E_2 schneidet die zu P_2 gehörige Tangentialebene T_2 in einer Geraden l_2, welche die Fläche in einen Punkt Q_2 schneidet, dessen Koordinaten zu K gehören und konjugiert zu denjenigen von Q_1 sind. Die Gerade l_3 durch Q_1 und Q_2 schneidet dann die Fläche in einem rationalen Punkt Q. Dieser ist verschieden von P. Fielen nämlich P und Q zusammen, so lägen die Geraden l und l_3 in derselben Ebene, die dann sowohl mit E_1 wie E_2 identisch sein müßte; dies ist unmöglich, da ja E_1 und E_2 verschieden sind.

Andererseits ist klar: Wenn E_1 mit rationalen Koeffizienten gewählt wird, so sind E_1 und E_2 identisch $(-E)$, und dann fallen P und Q zusammen; denn in der Ebene E wird die Schnittkurve mit der Fläche, wie oben bemerkt, in P einen Wendepunkt haben, und man erkennt dann aus der bekannten Parameterdarstellung der Schnittkurve mittels elliptischer Funktionen, daß Q mit P zusammenfallen muß. Nun können wir die Ebenen E_1 und E_2 so wenig verschieden wählen als wir wünschen, indem wir nämlich ihre Koeffizienten in K beliebig nahe an rationale Zahlen wählen. Dann muß der Punkt Q beliebig nahe an P heranrücken. Dies liefert die Existenz unendlich vieler rationaler Punkte auf der kubischen Fläche.

Das in diesem Beweis angewandte Verfahren habe ich auch benutzt zur Herleitung von Polynomlösungen in r von Gleichungen der Form $f(x, y, z) = r$ [vgl. die Bemerkung über (2) in § 2]. Zuerst kann man für eine kubische Form $f(x, y, z, u)$ mit rationalen Koeffizienten den Satz aufstellen:

Sind a_1, b_1, c_1, d_1 rationale Zahlen derart, daß $f(a_1, b_1, c_1, d_1) = 0$, während (a_2, b_2, c_2, d_2) ein Punkt auf der Schnittkurve ist zwischen der Fläche $f(x, y, z, u) = 0$ und ihrer Tangentenebene in (a_1, b_1, c_1, d_1), so ist

$$f(a_1 r + a_2,\ b_1 r + b_2,\ c_1 r + c_2,\ d_1 r + d_2) = h r,$$

wo h eine rationale Zahl ist.

Die Richtigkeit dieser Behauptung sieht man sofort wegen der TAYLOR-Entwicklung

$$f(a_1 r + a_2,\ b_1 r + b_2,\ c_1 r + c_2,\ d_1 r + d_2) = f(a_1, b_1, c_1, d_1)\, r^3 +$$
$$+ \left(\frac{\partial f}{\partial x}(a_1, b_1, c_1, d_1)\, a_2 + \frac{\partial f}{\partial y}(a_1, b_1, c_1, d_1)\, b_2 + \frac{\partial f}{\partial z}(a_1, b_1, c_1, d_1)\, c_2 + \right.$$
$$\left. + \frac{\partial f}{\partial u}(a_1, b_1, c_1, d_1)\, d_2 \right) r^2 + \left(\frac{\partial^2 f}{\partial x^2}(a_1, b_1, c_1, d_1)\, \frac{a_2^2}{2} + \cdots \right) r + f(a_2, b_2, c_2, d_2).$$

Hier verschwinden nämlich das erste, zweite und vierte Glied.

Als ein Beispiel sei die Form

$$x^3 + y^3 + 2z^3 + (x^2 + y^2 + 2z^2)\, u$$

gewählt. Hier können wir z.B.

$$a_1 = 1, \quad b_1 = 1, \quad c_1 = -1, \quad d_1 = 0$$

setzen. Die Tangentialebene in diesem Punkte hat die Gleichung

$$3x + 3y + 6z + 4u = 0.$$

Wählt man die Tangente, für welche

$$u = x - y$$

ist, so findet man den Schnittpunkt

$$a_2 = 5, \quad b_2 = 167, \quad c_2 = 22, \quad d_2 = -162.$$

Man erhält also hier die Identität

$$(r+5)^3 + (r+167)^3 + 2(-r+22)^3 -$$
$$- \left((r+5)^2 + (r+167)^2 + 2(-r+22)^2\right) 162 = 2 \cdot 3^9 r,$$

oder mit anderen Worten: Man findet, daß

$$x = \frac{r+5}{162}, \qquad y = \frac{r+167}{162}, \qquad z = \frac{-r+22}{162}$$

eine Lösung der inhomogenen Gleichung

$$x^3 + y^3 + 2z^3 - x^2 - y^2 - 2z^2 = \frac{1}{108} r$$

ist.

Von dieser Lösung aus können wir dann durch Tangenten- oder Sekantenziehung weitere Polynomlösungen ableiten, auch wenn man will mit mehr Parametern $s_1, s_2, \ldots$. Es hat kaum einen Zweck, darauf näher einzugehen.

Ich will mich hier damit begnügen, einige Ergebnisse mitzuteilen, die ich beim Studium der Gleichungen

$$xy(x+y)+z^3=ru^3 \tag{19}$$

$$x^3+y^2+z^2=r \tag{20}$$

$$x^3+y^3+z^2=r \tag{21}$$

$$x^3+y^3+z^3=ru^3 \tag{22}$$

erhalten habe. Für (19) habe ich sowohl die Lösung

$$x=12^3r,\quad y=-r^4+142r^2-864r+1331,\quad z=-12r^3+636r,$$
$$u=-60r^2+1452$$

wie auch

$$x=18^3r,\quad y=(r+1)(r^2-34r-1331),\quad z=-108r(r-35),$$
$$u=18(r^2-94r+121)$$

gefunden. Eine Lösung von (20) ist

$$x=1/4(-r^2+2r-2),\quad y=1/8(-r^2+6r+2),$$
$$z=1/8(-r^3+3r^2-4r-2).$$

Lösungen von (21) sind

$$x=-1/27(r+27),\quad y=1/27(r-54),\quad z=1/9(r+27)$$

und

$$x=-1/63(27r-26),\quad y=1/63(27r-47),\quad z=1/63(27r+37).$$

Was (22) betrifft, möchte ich etwas näher darauf eingehen, wie ich eine Lösung erhalten habe mit Hilfe des Verfahrens, das ich oben benutzt habe, um unendlich viele rationale Lösungen abzuleiten, ausgehend von einem Punkt, dessen zugehörige Tangentialebene die Fläche in drei kubisch irrationalen konjugierten Geraden schneidet. Im Falle der Gl. (22) ist P mit den Koordinaten $-1, 0, 1, 0$ ein solcher Punkt. Die Gerade

$$2y=x+z$$

geht durch P und schneidet die Fläche (22) in den beiden folgenden Punkten P_1 und P_2:

$$P_1:\quad x=1/3(1+2\sqrt{-2}),\quad y=1/3(2+\sqrt{-2}),\quad z=1,\quad u=0$$
$$P_2:\quad x=1/3(1-2\sqrt{-2}),\quad y=1/3(2-\sqrt{-2}),\quad z=1,\quad u=0.$$

Die Tangentenebene in P_1 ist

$$1/9(-7+4\sqrt{-2})x+1/9(2+4\sqrt{-2})y+z=0.$$

Ich wähle für l_1 die Schnittgerade dieser Ebene und der Ebene

$$4u=\sqrt{-2}(x-2y+z).$$

Man findet dann nach einiger Rechnung, daß l_1 die Fläche in den Punkt Q_1 mit den Koordinaten $x:y:z:u=$

$$\left(1+8\sqrt{-2}+r\left(4+2\sqrt{-2}\right)\right):\left(-10\sqrt{-2}+4r\right):$$
$$:\left(-1+8\sqrt{-2}+r\left(4-2\sqrt{-2}\right)\right):-18.$$

schneidet. Die Gerade zwischen Q_1 und dem konjugierten Punkt Q_2 kann dann dargestellt werden durch die Gleichung

$$x:y:z:u=\left(1+4t+r(4+t)\right):(-5t+4r):\left(-1+4t+r(4-t)\right):-18.$$

Also bekommt man für die Schnittpunkte mit der Fläche die Gleichung

$$\left(1+4t+r(4+t)\right)^3+(-5t+4r)^3+\left(-1+4t+r(4-t)\right)^3+18^3r=0,$$

wobei zwei der Wurzeln $2\sqrt{-2}$ und $-2\sqrt{-2}$ sind. Man findet, daß die dritte Wurzel $(-24r^3-732r)/(24r+3)$ ist. Die Einsetzung hiervon liefert den Punkt Q mit Koordinaten

$$x:y:z:u=(-8r^4-236r^2-972r+1):(72r^3+1224r):$$
$$:(8r^4+236r^2-972r-1):-18(8r^2+1),$$

wodurch eine Polynomlösung von (22) gefunden ist.

Bekanntlich hat Richmond auf Grund einer früheren Arbeit von Ryley bewiesen, daß für $r>0$ positive rationale Lösungen x, y, z der Gleichung

$$x^3+y^3+z^3=r$$

existieren. Seine Methode besteht in rechnerischen Kunstgriffen (vgl. Hardy and Wright [1], S. 196—198). Es bietet keine Schwierigkeit, mittels wiederholter Tangentenziehung positive rationale Lösungen der oben erwähnten Gleichungen zu finden, wenn man überhaupt rationale Lösungen gefunden hat; ich will aber hier nicht näher darauf eingehen.

Literatur.

[1] Hardy, G. H., and E. M. Wright: An Introduction to the Theory of Numbers 1938. — [2] Hasse, H.: Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II: Reziprozitätsgesetz. Jber. dtsch. Math.-Ver., Erg.-Bd. **6** (1930). — [3] Mordell, L. J.: Rational points on cubic surfaces. Publ. Math. Debrecen **1**, 1—6 (1949). — [4] Segre, B.: A parametric solution of the indeterminate cubic equation $z^2=f(x, y)$. J. London Math. Soc. **18**, 226—233 (1943). — [5] Segre, B.: On arithmetical properties of singular cubic surfaces. J. London Math. Soc. **19**, 84—91 (1944). — [6] Selmer, E. S.: Sufficient congruence conditions for the existence of rational points on certain cubic surfaces. Math. Scand. **1**, 113—119 (1953). — [7] Skolem, Th.: Diophantische Gleichungen. Erg. Math. **5**, H. 4 (1938). — [8] Skolem, Th.: On the existence of a multiplicative basis for an arbitrary algebraic field. Det Kong. Norske Vidensk. Selsk., Forh. **20**, Nr. 2 (1947).

Guldbergs vei 4, Smestad, Oslo (Norwegen).

(Eingegangen am 16. April 1955.)

Hahn, W.
Math. Zeitschr. Bd. 63, S. 313—319 (1955)

Über analytische Lösungen linearer Differential-Differenzengleichungen.

Issai Schur zum Gedächtnis.

Von

Wolfgang Hahn.

1. Wir betrachten im folgenden die Lösungen einer linearen Differential-Differenzengleichung

$$\sum_{i=0}^{p} a_i Y^{(i)}(t) + \sum_{i=0}^{q} b_i Y^{(i)}(t-1) = 0 \qquad (p \geqq q) \tag{1}$$

mit komplexen Koeffizienten a_i, b_i. Da das Studium derartiger Gleichungen vornehmlich durch technische Fragestellungen angeregt worden ist, in denen die Zeit als unabhängige Veränderliche t auftritt, hat man bisher fast ausschließlich die Lösungen als Funktionen einer reellen Veränderlichen untersucht. Analytische Lösungen von (1) sind bisher nur von Herrn Leontev[1]) behandelt worden. Die nachstehende Arbeit beschäftigt sich ebenfalls mit analytischen Lösungen, und zwar in dem Sonderfall $p > q$, in dem die Verhältnisse viel einfacher sind als in dem allgemeinen Fall $p \geqq q$. Die Ergebnisse liegen aber in anderer Richtung als die Leontevschen [bis auf die Formel (9), die auch bei Leontev steht]; es handelt sich vor allem um das Verhalten gewisser unendlicher Reihen auf der Grenze ihres Konvergenzbereichs, um die Übertragung der klassischen Sätze von Abel und Tauber und um den Nachweis der Existenz singulärer Punkte.

Mit $C_1, C_2, \ldots$ sind im folgenden positive Konstanten bezeichnet, auf deren genauen Wert es nicht weiter ankommt.

2. Aus der Theorie der Gl. (1) im Reellen benötigen wir die folgenden Ergebnisse[2]).

a) Die Gleichung hat unendlich viele Partiallösungen der Gestalt

$$Y_j(t) = e^{r_j t} \qquad (j = 1, 2, \ldots). \tag{2}$$

Dabei sind die Zahlen r_j die Nullstellen der „charakteristischen Funktion"

$$A(r) = \sum_{i=0}^{p} a_i r^i + e^{-r} \sum_{i=0}^{q} b_i r^i. \tag{3}$$

[1]) Leontev, A. F.: Differential-Differenzengleichungen. Mat. Sbornik **24** (66), 347 bis 374 (1949) [Russisch]. Eine kurze Zusammenstellung der Hauptergebnisse steht bei Hahn, W.: Bericht über Differential-Differenzengleichungen mit festen und veränderlichen Spannen. Jber. dtsch. Math.-Ver. **57**, 55—84 (1954).

[2]) Wright, E. M.: The linear difference-differential equation with constant coefficients. Proc. Roy. Soc. Edinburgh A **62**, 387—393 (1949).

Wenn r_k m-fache Nullstelle von $A(r)$ ist, sind auch die Funktionen

$$t\,e^{r_k t},\ t^2 e^{r_k t},\ \ldots,\ t^{m-1} e^{r_k t} \tag{4}$$

Lösungen von (1). Es können aber höchstens endlich viele Mehrfachnullstellen auftreten.

b) Jede für reelle positive t erklärte Lösung von (1) läßt sich als lineare Verbindung der Partiallösungen (2) bzw. (4) darstellen, also in der Gestalt

$$f(t) = \sum_{j=1}^{\infty} A_j(t)\, e^{r_j t}. \tag{5}$$

Die Ausdrücke $A_j(t)$ sind im allgemeinen Konstanten und nur für endlich viele Indizes, die den Mehrfachnullstellen entsprechen, Polynome.

c) Ordnet man die Nullstellen von $A(r)$, die positiven Imaginärteil haben — sie sollen nachstehend durch $s_n = u_n + i v_n$ bezeichnet werden — nach wachsenden Beträgen, so gilt für große n eine asymptotische Darstellung[3])

$$s_n = -(p-q)\log n + C_1 + C_2 n i + C_3 i + R_n. \tag{6}$$

Das Restglied R_n genügt einer Abschätzung

$$|R_n| < C_4 \frac{\log n}{n}. \tag{7}$$

Die asymptotische Darstellung (6) gilt sinngemäß auch für die Nullstellen mit negativem Imaginärteil.

3. Da sich jede Lösung der Funktionalgleichung, die für $t > 0$ erklärt ist, als Reihe der Form (5) darstellen läßt, gilt dies auch für jede analytische Lösung; denn man kann durch eine lineare Transformation der Variablen, die die Form der Reihe (5) ungeändert läßt, stets erreichen, daß die Funktion in einem Intervall der positiven reellen Achse regulär ist. Die Partiallösungen (2) und (4) sind natürlich ganze Funktionen. Wir betrachten deshalb nur unendliche Reihen und beschränken uns zunächst auf Nullstellen s_n mit positivem Imaginärteil v_n:

$$f(z) = \sum_{n=1}^{\infty} A_n\, e^{s_n z}. \tag{8}$$

Die unabhängige Variable, die jetzt komplex ist, ist mit z bezeichnet, die A_n sind beliebige komplexe Zahlen. Von den endlich vielen Mehrfachnullstellen ist abgesehen, da die ihnen entsprechenden Partiallösungen (4) auf das analytische Verhalten der Funktion keinen Einfluß haben. Es wird sich zeigen, daß sich die Reihen (8) in mancher Hinsicht wie Dirichletsche Reihen verhalten. Sie konvergieren, wenn sie nicht eine ganze Funktion darstellen, in einer Halbebene, die durch eine Konvergenzhorizontale nach unten begrenzt wird. Bei Annäherung an Punkte dieser Geraden gilt ein Satz vom Abelschen Typ — aus dem man folgern kann, daß die Reihe in der offenen

[3]) LANGER, R. E.: The asymptotic location of the roots of a certain transcendental equation. Trans. Amer. Math. Soc. **31**, 837—844 (1929).

Halbebene eine analytische Funktion darstellt — und unter Zusatzannahmen über die Koeffizienten ein Satz vom Tauberschen Typ. Mit seiner Hilfe kann man unter gewissen Voraussetzungen über die Koeffizienten die Existenz singulärer Punkte auf der Konvergenzgeraden zeigen.

4. Bestimmung des Konvergenzgebiets. Es sei

$$a = \limsup_{n\to\infty} \frac{\log |A_n|}{v_n} \qquad (s_n = u_n + i v_n). \tag{9}$$

Dann konvergiert die Reihe (8) *für* $Im\, z > a$ *absolut und divergiert für* $Im\, z < a$.

Der *Beweis* verläuft wie der des entsprechenden Satzes über Dirichlet-Reihen. Gibt man $\varepsilon > 0$ beliebig klein vor, so ist nach (9) zuletzt $\log |A_n| \leqq (a+\varepsilon) v_n$ und unendlich oft $\log |A_n| > (a-\varepsilon) v_n$. Nun sei $z = x + i y$. Dann ist für hinreichend große n

$$|A_n e^{s_n z}| \leqq e^{a v_n} e^{\varepsilon v_n} e^{u_n x - v_n y}.$$

Wählt man $y > a$ und $0 < \varepsilon < y - a$, also etwa $y = a + \varepsilon + b$ mit $b > 0$, so ist

$$|A_n e^{s_n z}| \leqq e^{u_n x - b v_n}.$$

Aus (6) ergibt sich, daß die rechte Seite dieser Ungleichung in der Form

$$C_5 n^{-(p-q)x} e^{-C_2 b n}(1 + R_n')$$

geschrieben werden kann; für R_n' gilt eine Abschätzung wie (7). Da $C_2 b > 0$ ist, ist die Reihe mit dem allgemeinen Glied $A_n e^{s_n z}$ absolut konvergent. Ist aber $y < a$, etwa $y = a - 2\varepsilon$, $\varepsilon > 0$, so ist unendlich oft

$$|A_n e^{s_n (x+iy)}| > e^{(a-\varepsilon) v_n + u_n x + 2\varepsilon v_n - a v_n} = e^{u_n x + \varepsilon v_n},$$

und das strebt gegen unendlich.

Über das Verhalten der Reihe auf der Konvergenzhorizontalen (KH) gilt: *Es sei*

$$c = \limsup_{n\to\infty} \frac{\log |A_n| - a v_n}{-u_n}. \tag{10}$$

Dann konvergiert die Reihe $f(z)$ *auf der Halbgeraden* $z = x + i a$, $x > c + \frac{1}{p-q}$, *absolut und divergiert für* $x < c$.

Beweis. Man erkennt wie eben, daß zuletzt für jedes $c' > c$

$$|A_n e^{s_n (x+ia)}| = |A_n|\, |e^{u_n x - a v_n}| \leqq e^{u_n (x - c')}$$

ist. Wegen (6) ist

$$e^{u_n (x-c')} = C_6 n^{-(p-q)(x-c')}(1 + R_n'');$$

die Reihe konvergiert daher absolut, wenn $(x-c')(p-q) > 1$ bzw., da das für alle $c' > c$ gelten soll, wenn $(x-c)(p-q) > 1$ ist. Wenn andererseits $f(z)$ für den Punkt $z_0 = x_0 + i y_0$ der KH konvergiert, so ist sicher $A_n e^{s_n z_0}$ beschränkt, $|A_n e^{s_n z_0}| < M$. Dann wird

$$|f(z)| = \left| \sum_{n=1}^{\infty} A_n e^{s_n z_0} e^{s_n (z - z_0)} \right| \leqq M \sum_{n=1}^{\infty} |e^{s_n (z - z_0)}|.$$

Wenn $Im(z-z_0)>0$ ist, konvergiert die rechtsstehende Reihe; das liefert nichts Neues. Ist $Im(z-z_0)=0$, d.h. liegt z auf der KH, so konvergiert die Reihe im Fall $Re(z-z_0)>\frac{1}{p-q}$ absolut. Das Intervall, in dem Punkte bedingter Konvergenz auftreten, kann also höchstens die Länge $\frac{1}{p-q}$ haben.

Die durch (9) und (10) definierten Zahlen können auch unendlich große Werte annehmen, wie aus der folgenden Zusammenstellung hervorgeht.

A_n	a	c
e^{n^2}	$+\infty$	$-$
e^{-n^2}	$-\infty$	$-$
$e^{-\sqrt{n}}$	0	$-\infty$
1	0	0
$n^{\log n}$	0	$+\infty$

An der Stelle $z=c$ kann Konvergenz oder Divergenz vorliegen, wie die Beispiele $A_n=1$ und $A_n=\frac{(-1)^n}{\log n}$ zeigen. In beiden Fällen ist $c=0$; während die erste Reihe divergiert, konvergiert die zweite nach dem Leibnizschen Kriterium.

5. Satz vom Abelschen Typus. *Es sei $f(z)$ an der Stelle $z=z_0$ der KH konvergent. Dann konvergiert die Reihe gleichmäßig in jedem Winkelraum mit dem Scheitelpunkt z_0, dessen Öffnung kleiner als π ist und der ganz der oberen Halbebene angehört.*

Für den Beweis führen wir die folgenden Abkürzungen ein:

$$z-z_0=\zeta=\xi+i\eta, \qquad b_k=e^{s_k\zeta},$$

$$a_{m,k}=\sum_{j=m}^{k}A_j e^{s_j z_0}, \quad \text{also} \quad A_k e^{s_k z_0}=a_{m,k}-a_{m,k-1} \qquad (k>m),$$

$$\sigma_{m,M}=\sum_{k=m+1}^{m+M}A_k e^{s_k z}=\sum_{k=m+1}^{m+M}A_k e^{s_k z_0} b_k.$$

Durch partielle Summation erhält man

$$\sigma_{m,M}=a_{m,m+M}\,b_{m+M}-\sum_{t=m+1}^{m+M-1}a_{m,t}(b_{t+1}-b_t).$$

Da $f(z_0)$ konvergiert, gehen die Teilsummen $a_{m,k}$ mit $m\to\infty$ gleichmäßig bezüglich k gegen Null, d.h. es ist

$$|a_{m,m+M}|<B_m \quad \text{mit} \quad \lim B_m=0 \quad \text{für} \quad m\to\infty.$$

Daher wird

$$|\sigma_{m,M}|\leq B_m|b_{m+M}|+B_m\sum_{t=m+1}^{m+M-1}|b_{t+1}-b_t|,$$

und der Nachweis der gleichmäßigen Konvergenz der Reihe $f(z)$ ist erbracht, wenn gezeigt worden ist, daß die Reihe

$$\sum_{t=m+1}^{\infty} |b_{t+1} - b_t| \tag{11}$$

innerhalb des Winkelraums gleichmäßig konvergiert. Es ist

$$b_{t+1} - b_t = e^{s_t \zeta} (e^{(s_{t+1} - s_t)\zeta} - 1). \tag{12}$$

Die Klammer schätzen wir nach der Formel

$$|1 - e^w| = \left| \int_0^w e^x \, dx \right| \leqq |w|$$

ab, die im Fall $Re\, w < 0$ gilt und hier angewandt werden darf, da

$$Re\,[(s_{t+1} - s_t)\zeta] = (u_{t+1} - u_t)\,\xi - (v_{t+1} - v_t)\,\eta$$

mit Rücksicht auf (6) für große t sicher negativ ist. Ferner ist

$$|e^{s_t \zeta}| = e^{u_t \xi - v_t \eta}.$$

Im Winkelraum ist

$$\eta \geqq C_7 |\xi|,$$

und wieder wegen (6) ist für große t

$$u_t \xi - v_t \eta < - C_8 t \eta,$$

also

$$|e^{s_t \zeta}| < e^{-C_8 t \eta}.$$

Setzt man das alles in (12) ein, so folgt

$$|b_{t+1} - b_t| < |\zeta|\,|s_{t+1} - s_t|\, e^{-C_8 t \eta}.$$

Ferner ist im Winkelraum $|\zeta| \leqq C_9 \eta$. Beachtet man noch, daß $s_{t+1} - s_t$ beschränkt ist, so folgt schließlich

$$|b_{t+1} - b_t| < C_{10} \eta\, e^{-C_8 t \eta}.$$

Summiert man nun über alle hinreichend großen t, so erhält man für die Reihe (11) eine Abschätzung

$$\sum_{t=m+1}^{\infty} |b_{t+1} - b_t| < C_{11} \frac{\eta}{1 - e^{-C_8 \eta}}.$$

Die rechte Seite der Ungleichung hat für $\eta \to 0+$, was der Annäherung von z gegen z_0 innerhalb des Winkelraums entspricht, einen endlichen Grenzwert. Damit ist der Beweis erbracht.

Aus dem Satz ergibt sich, daß $f(z)$ bei Annäherung an einen Konvergenzpunkt stetig ist, sofern die Annäherung im Winkelraum stattfindet. Es ergibt sich weiter, daß die Reihe $f(z)$ in jeder Halbebene $Im\, z \geqq a' > a$ eine analytische Funktion darstellt.

Wenn z_0 ein Punkt absoluter Konvergenz ist, kann man noch die rechts von z_0 gelegene Hälfte der KH in den Winkelraum mit einbeziehen. Es ist ja dann

$$|f(z)| = \left|\sum_{n=1}^{\infty} A_n e^{s_n z_0} e^{s_n \zeta}\right| \leq \sum_{n=1}^{\infty} |A_n e^{s_n z_0}|\,|e^{s_n \zeta}|.$$

Im Winkelraum ist $e^{s_n \zeta}$ beschränkt, wenn ζ beschränkt bleibt; man kann also $f(z)$ durch eine absolut konvergente Reihe majorisieren.

6. Satz vom Tauberschen Typ. *Es sei die durch* (12) *erklärte Zahl* $a=0$, *also* $f(z)=\sum_{n=1}^{\infty} A_n e^{s_n z}$ *für* $Im\, z>0$ *konvergent; es sei* $\lim_{n\to\infty} n A_n = 0$. *Es sei* $\lim f(x_0+iy)$ *für* $y\to 0+$, *also für Annäherung von oben her, vorhanden und gleich L. Dann konvergiert* $\sum_{n=1}^{\infty} A_n e^{s_n x_0}$ *gegen den Wert L.*

Man kann ohne Beschränkung der Allgemeinheit $x_0=0$ annehmen. Aus der Zusatzbedingung folgt dann $c=-\frac{1}{p-q}$ und die absolute Konvergenz der Reihe für reelles $z=x>0$, da sich $|e^{s_n x}|$ wie $n^{-x(p-q)}$ verhält und A_n schneller als n^{-1} abnimmt. Der Beweis verläuft wie der des klassischen Tauberschen Satzes[4]). Es sei

$$S_n = \sum_{t=1}^{n} A_t,$$

so daß

$$|S_n - f(iy)| = \sum_{t=1}^{n} A_t(1-e^{s_t iy}) - \sum_{t=n+1}^{\infty} A_t e^{s_t iy} \leq \sum_{t=1}^{n} |A_t|\,|1-e^{s_t iy}| + \sum_{t=n+1}^{\infty} |A_t|\,|e^{s_t iy}|$$

wird. Da $Re(s_t iy)$ negativ ist, kann man wie oben im Anschluß an (12)

$$|1-e^{s_t iy}| \leq |s_t|\, y \leq C_{12}\, t\, y$$

schließen. Ferner ist

$$|e^{s_t iy}| = e^{-v_t y} \leq e^{-C_{13} t y}$$

mit passendem C_{13}. Es sei $M_n = \operatorname{Max}_{t>n} |A_t|$ und $M_n' = \operatorname{Max}_{t>n} |tA_t|$. Aus der Zusatzbedingung über die Koeffizienten folgt dann

$$M_n < M_n' n^{-1},$$

und man erhält

$$|S_n - f(iy)| \leq C_{12}\, y \sum_{t=1}^{n} t\,|A_t| + M_n' n^{-1} \sum_{t=n+1}^{\infty} |e^{-C_{13} t y}|.$$

Nun läßt man y die Folge n^{-1} durchlaufen. Dann ist wegen $t|A_t|\to 0$ auch

$$\lim_{n\to\infty} \sum_{t=1}^{n} t \frac{A_t}{n} = 0.$$

[4]) LANDAU, E.: Darstellung und Begründung einiger neuerer Ergebnisse der Funktionentheorie. § 8.

Ferner ist

$$\lim_{n\to\infty} n^{-1} \sum_{t=n+1}^{\infty} \left| e^{-C_{13} t y} \right| = \lim_{\frac{1}{n}\to 0} \frac{\frac{1}{n} \cdot e^{-C_{13}\left(1+\frac{1}{n}\right)}}{1 - e^{-C_{13}\cdot\frac{1}{n}}}$$

endlich, und da M_n' gegen Null geht, folgt $\lim_{n\to\infty} S_n - f\left(\frac{i}{n}\right) = \lim_{n\to\infty} |S_n - L| = 0$ und damit die Behauptung.

7. Existenz singulärer Punkte. Eine unmittelbare Folge aus Nr. 6 ist der Satz: *Es sei* $a = 0$, $nA_n \to 0$ *und* $\sum_{n=1}^{\infty} A_n$ *divergent. Dann ist der Punkt* $z = 0$ *singulär.* Andernfalls müßte ja $\lim f(iy)$ für $y \to 0$ existieren, und nach dem „Tauberschen" Satz wäre $\sum_{n=1}^{\infty} A_n$ konvergent. Aus der Funktionalgleichung (1) folgert man in diesem Fall auch die Singularität der Punkte $z = 1, 2, \ldots$. Die Voraussetzung ist z.B. für $A_n = \frac{1}{n \log n}$ erfüllt.

8. Die Betrachtungen der letzten vier Nummern lassen sich auf Lösungen der Form

$$g(z) = \sum_{n=1}^{\infty} A_n' e^{s_n' z} \tag{16}$$

übertragen, worin s_n' die Nullstellen mit negativem Imaginärteil durchläuft. Diese Reihen konvergieren natürlich in „unteren" Halbebenen. Die Lösungen der Form (5) konvergieren, wenn sie überhaupt analytische Funktionen darstellen, in Horizontalstreifen; denn — vgl. [2]) — sie konvergieren für hinreichend große reelle t absolut, lassen sich daher als Summe einer Reihe (8) und einer Reihe (16) schreiben. Eine solche Summe ist also die allgemeinste Form einer analytischen Lösung der Funktionalgleichung (1). Ob die betrachteten Reihen über die Konvergenzhorizontalen analytisch fortsetzbar sind oder nicht — wobei auch die Möglichkeit besteht, daß die fortgesetzten Reihen nicht mehr der Funktionalgleichung genügen — läßt sich aus den abgeleiteten Sätzen nicht entnehmen.

Braunschweig, Mathematisches Institut der Technischen Hochschule.

(Eingegangen am 16. April 1955.)

GRUNSKY, H.
Math. Zeitschr. Bd. 63, S. 320—323 (1955)

Eine funktionentheoretische Integralformel.

Von

HELMUT GRUNSKY.

Meinem verehrten Lehrer ISSAI SCHUR zum Gedächtnis.

Der GAUSSsche Integralsatz kann als ein Analogon zu der Grundformel der Differential- und Integralrechnung angesehen werden: Wie diese das Integral über die Ableitung einer Funktion durch ihre Werte am Rande des Intervalles darstellt, so wird im GAUSSschen Integralsatz das Gebietsintegral über die Divergenz eines Vektorfeldes durch das Feld am Rande, d.h. jetzt durch ein Rand*integral*, ausgedrückt. Entsprechendes gilt für den STOKESschen Satz, der ja übrigens in dem uns hier allein interessierenden Fall der Ebene nichts Neues gegenüber dem GAUSSschen enthält. Es soll im folgenden gezeigt werden, daß sich in gewissen Fällen (auch wenn man von dem bekannten trivialen absieht, bei dem $\iint u_{xy}\,dx\,dy$ über ein achsenparalleles Rechteck betrachtet wird) die Integration noch einen Schritt weiter treiben läßt, so daß sich ein Gebietsintegral durch eine endliche Summe von Randwerten ausdrücken läßt. Das trifft nämlich zu für das Integral einer analytischen Funktion, erstreckt über ein Polygongebiet; es ist darstellbar durch eine Linearkombination der Werte der zweiten Stammfunktion in den Ecken mit Koeffizienten, die durch das Polygon allein bestimmt sind. Der einfache Beweis stützt sich auf eine Formulierung des GAUSS-STOKESschen Satzes mit den Darstellungsmitteln der komplexen Analysis, die zwar nicht neu[1]), aber doch nicht gerade geläufig ist. Ich beginne daher mit einem knappen Beweis dieser Formel.

Es sei $\mathfrak{f}(z)$ eine stetig differenzierbare, komplexwertige Funktion der komplexen Veränderlichen $z = x + iy$ in dem Gebiet $\mathfrak{G}$. Wir erklären auf dem System der BORELschen Teilmengen $\mathfrak{B} \subset \mathfrak{G}$ eine komplexwertige, totalstetige, abzählbar additive Mengenfunktion $\mathfrak{F}(\mathfrak{B})$, indem wir zunächst für ein beliebiges halboffenes Intervall $I \subset \mathfrak{G}: x_0 \leqq x < x_1,\ y_0 \leqq y < y_1$ setzen:

$$\mathfrak{F}(I) = \int_{\mathrm{Rd}\, I} \mathfrak{f}(z)\, dz \tag{1}$$

und dann $\mathfrak{F}$ in bekannter Weise erweitern. Ist $\mathfrak{C}$ eine kompakte Teilmenge von $\mathfrak{G}$, deren Rand aus einem System C von endlich vielen einfach geschlossenen, rektifizierbaren Kurven besteht, so ist

$$\mathfrak{F}(\mathfrak{C}) = \int_{C} \mathfrak{f}(z)\, dz. \tag{2}$$

[1]) Vgl. z.B. BERGMANN, ST.: The kernel function and conformal mapping, p. 57 New York 1950.

$\mathfrak{F}(\mathfrak{B})$ hat eine Dichte, die wir ermitteln wollen. Wir schreiben die Formel für das totale Differential von $\mathfrak{f}(z)$ in der Form

$$(3) \qquad \mathfrak{f}(z) = \mathfrak{f}(z_0) + \mathfrak{f}_z(z_0)\cdot(z - z_0) + \mathfrak{f}_{\bar z}(z_0)\cdot(\bar z - \bar z_0) + o(|z - z_0|),$$

wobei die Koeffizienten $\mathfrak{f}_z(z_0)$ und $\mathfrak{f}_{\bar z}(z_0)$ eben durch diese Formel definiert sind. Die Umrechnung des in reellen Koordinaten geschriebenen totalen Differentials auf (3) ergibt den folgenden Zusammenhang mit $\mathfrak{f}_x = \frac{\partial \mathfrak{f}}{\partial x}$, $\mathfrak{f}_y = \frac{\partial \mathfrak{f}}{\partial y}$:

$$\mathfrak{f}_z = \frac{\partial \mathfrak{f}}{\partial z} = \frac{1}{2}\left(\frac{\partial \mathfrak{f}}{\partial x} - i\,\frac{\partial \mathfrak{f}}{\partial y}\right), \qquad \mathfrak{f}_{\bar z} = \frac{\partial \mathfrak{f}}{\partial \bar z} = \frac{1}{2}\left(\frac{\partial \mathfrak{f}}{\partial x} + i\,\frac{\partial \mathfrak{f}}{\partial y}\right).$$

Ist $\mathfrak{f}(z)$ speziell analytisch, so ersieht man aus (3) die identische Gültigkeit der Gleichung $\mathfrak{f}_{\bar z}(z) = 0$, und diese ist kennzeichnend für analytische Funktionen. Sie ist nichts anderes als eine besondere Schreibweise der Cauchy-Riemannschen Differentialgleichungen. Ferner ist für ein analytisches $\mathfrak{f}(z)$:

$$\mathfrak{f}_z(z) = \mathfrak{f}'(z).$$

Setzen wir (3) in (1) ein, so ergeben die beiden ersten Glieder den Beitrag 0, das Restglied ein $o(|z_1 - z_0|^2)$, das dritte Glied dagegen

$$\mathfrak{f}_{\bar z}(z_0) \int\limits_{\mathrm{Rd}\,I} \bar z\, dz = 2i\, I\cdot \mathfrak{f}_{\bar z}(z_0),$$

wo I jetzt den Inhalt des Intervalles bedeutet. Läßt man nun z_1 nach z_0 rücken, so erkennt man, daß die Dichte von $\mathfrak{F}(\mathfrak{B})$ gleich $2i\,\mathfrak{f}_{\bar z}$ ist. Es folgt unmittelbar:

$$(4) \qquad \int\limits_C \mathfrak{f}(z)\, dz = 2i \iint\limits_{\mathfrak{C}} \frac{\partial \mathfrak{f}}{\partial \bar z}\,(dz),$$

wo (dz) ein Flächenelement bezeichnet und C und $\mathfrak{C}$ dieselbe Bedeutung wie in (2) haben. — Diese Formel geht für analytische $\mathfrak{f}(z)$ in den Cauchyschen Integralsatz über. Zerlegt man (4) in Real- und Imaginärteil, so findet man den Stokesschen und den Gaussschen Integralsatz für das Vektorfeld $\overline{\mathfrak{w}} = \overline{\mathfrak{f}(z)}$.

Gehen wir in (4) beiderseits zum konjugiert Komplexen über und schreiben statt $\overline{\mathfrak{f}(z)}$ wieder $\mathfrak{f}(z)$, so erhalten wir:

$$\iint\limits_{\mathfrak{C}} \frac{\partial \mathfrak{f}}{\partial z}\,(dz) = \frac{i}{2}\int\limits_C \mathfrak{f}(z)\, d\bar z.$$

Wir wollen nun diese Formel insbesondere auf eine analytische Funktion $\mathfrak{f}(z)$ anwenden. Setzen wir noch $\mathfrak{f}(z) = f'(z)$ so bekommen wir:

$$(5) \qquad \iint\limits_{\mathfrak{C}} f''(z)\,(dz) = \frac{i}{2}\int\limits_C f'(z)\, d\bar z.$$

Das Integral der rechten Seite läßt sich bei besonderen Voraussetzungen über C auswerten. Es sei insbesondere $\mathfrak{C} = \mathfrak{P}$ ein ein- oder mehrfach zusammenhängendes Polygongebiet mit Rand P und den Ecken z_ν, $\nu = 1, \ldots, n$; $z_{\nu+}$ sei

die bei einem positiven Umlauf auf z_ν folgende, $z_{\nu-}$ die vorangehende Ecke, P_ν die Seite $(z_\nu, z_{\nu+})$, deren Richtung durch ε_ν mit $|\varepsilon_\nu| = 1$ gekennzeichnet werde: $z_{\nu+} - z_\nu = \varepsilon_\nu |z_{\nu+} - z_\nu|$. Dann ist:

$$\int_{P_\nu} f'(z)\, d\bar{z} = \varepsilon_\nu^{-2} \int_{P_\nu} f'(z)\, dz = \varepsilon_\nu^{-2} \big(f(z_{\nu+}) - f(z_\nu)\big).$$

Summiert man über alle Polygonseiten und ordnet nach den $f(z_\nu)$, so drückt sich die rechte Seite von (5) als Linearverbindung dieser Größen aus, und man erhält:

$$\iint_{\mathfrak{P}} f''(z)\, (dz) = \sum_{\nu=1}^{n} \delta_\nu f(z_\nu) \tag{6}$$

mit

$$\delta_\nu = \frac{i}{2} (\varepsilon_{\nu-}^{-2} - \varepsilon_\nu^{-2}). \tag{7}$$

Wesentlich ist, daß die δ_ν durch das Polygon allein bestimmt und von $f(z)$ unabhängig sind.

Ein einfacher Grenzübergang erlaubt es schließlich, die Voraussetzung, daß $f(z)$ auch auf dem Rande des Polygongebietes regulär sei, durch die der Stetigkeit im abgeschlossenen Bereich zu ersetzen. — Somit ist bewiesen:

Satz. *$f(z)$ sei regulär in dem Gebiet des geradlinig berandeten, ein- oder mehrfach zusammenhängenden Polygons $\mathfrak{P}$ mit den Ecken z_ν $(\nu = 1, \ldots, n)$ und stetig in dem zugehörigen abgeschlossenen Bereich. Dann existiert die linke Seite von* (6) *und es gilt* (6) *mit* (7), *wo ε_ν mit $|\varepsilon_\nu| = 1$ die Richtung der von z_ν ausgehenden, $\varepsilon_{\nu-}$ die der in z_ν mündenden Polygonseite kennzeichnet.*

Die Analogie dieses Ergebnisses mit der Grundformel der Differential- und Integralrechnung ist offenkundig. Diese Analogie legt viele Anwendungsmöglichkeiten nahe, auf die ich an anderer Stelle eingehe[2]).

Von besonderer Wichtigkeit ist natürlich der Fall, daß $\mathfrak{P} = \mathfrak{D}$ ein Dreieck ist. Für die δ_ν gibt es dann eine andere zweckmäßige Darstellung, die man leicht unabhängig von (7) findet, wenn nur überhaupt die Gültigkeit einer Formel (6) bekannt ist. Wenden wir nämlich diese nacheinander auf $f(z) = 1$, $f(z) = z$, $f(z) = z^2$ an, so erhalten wir für die δ_ν, $\nu = 1, 2, 3$ die drei Gleichungen:

$$\sum \delta_\nu = 0, \qquad \sum z_\nu \delta_\nu = 0, \qquad \sum z_\nu^2 \delta_\nu = 2\mathfrak{D}$$

und damit

$$\delta_\nu = \frac{2\mathfrak{D}}{(z_\nu - z_{\nu-1})(z_\nu - z_{\nu+1})}, \tag{8}$$

wo die Indizes mod 3 zählen. Natürlich bestätigt man leicht die Übereinstimmung von (7) und (8).

Setzt man nun noch voraus $f(z_1) = f(z_2) = 0$ und schreibt z für z_3, für die Integrationsveränderliche dagegen ζ, so folgt als Darstellung der in zwei

[2]) Über eine Anwendung auf dem Gebiete der Differenzenrechnung habe ich auf dem Internationalen Mathematikerkongreß 1954, Amsterdam, berichtet. Vgl. Proc. Int. Congr. Math. **2**, 114—115 (1954).

gegebenen Punkten verschwindenden zweiten Stammfunktion zu einer gegebenen analytischen Funktion $f''(z)$:

$$f(z) = \frac{1}{2}(z - z_1)(z - z_2)\,\mathfrak{M}(f''(\zeta); z), \tag{9}$$

wo $\mathfrak{M}$ den Mittelwert von f'' über das Dreieck $\mathfrak{D}$ mit den Ecken z_1, z_2, z bedeutet:

$$\mathfrak{M}(f''(\zeta); z) = \frac{1}{\mathfrak{D}} \iint_{\mathfrak{D}} f''(\zeta)\,(d\zeta).$$

Falls z auf der Verbindungsstrecke von z_1 und z_2 liegt und diese Punkte (ohne Beschränkung der Allgemeinheit) als reell angenommen werden, so geht (9) in die bekannte Integraldarstellung einer Funktion $f(z)$ mit $f(z_1) = f(z_2) = 0$ mittels $f''(z)$ über:

$$f(z) = \int_{z_1}^{z_2} k(z, \zeta)\, f''(\zeta)\, d\zeta$$

mit

$$k(z, \zeta) = \begin{cases} \dfrac{(\zeta - z_1)(z - z_2)}{z_2 - z_1} & \zeta \leqq z \\ \dfrac{(\zeta - z_2)(z - z_1)}{z_2 - z_1} & \zeta \geqq z. \end{cases}$$

Aus (9) ergibt sich als unmittelbare Folgerung: Ist $f(z)$ regulär in einem konvexen Gebiet $\mathfrak{G}$ und ist $f(z_1) = f(z_2) = 0$, $|f''(z)| \leqq 1$, so gilt in $\mathfrak{G}$:

$$|f(z)| \leqq \frac{1}{2}\,|z - z_1| \cdot |z - z_2|.$$

Mainz, Mathematisches Institut der Universität.

(Eingegangen am 28. April 1955.)

SPECHT, W.
Math. Zeitschr. Bd. 63, S. 324—330 (1955)

Abschätzung der Wurzeln algebraischer Gleichungen. III.

ISSAI SCHUR zum Gedächtnis.

Von

WILHELM SPECHT.

Bestimmt man zu einem komplexen Polynom

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n \tag{1}$$

des Grades n die Größen

$$\alpha = \max_{1 \le \nu \le n} \sqrt[\nu]{|a_\nu|}, \tag{2.1}$$

$$\beta = \max_{1 \le \nu \le n} |a_\nu|, \tag{2.2}$$

so bestehen für die nach ihrem absoluten Betrage

$$|\xi_1| \ge |\xi_2| \ge \cdots \ge |\xi_n| \tag{3}$$

geordneten Nullstellen $\xi_1, \xi_2, \ldots, \xi_n$ des Polynoms Ungleichungen[1])

$$|\xi_1 \xi_2 \ldots \xi_k| < \sigma_k \alpha^k \quad \text{für} \quad 1 \le k \le n \tag{4}$$

mit den nur von der Stellenzahl k, nicht aber vom Grade n abhängigen Konstanten

$$\sigma_k = k^{-\frac{k}{2}} (k+1)^{\frac{k+1}{2}} \quad \text{für} \quad 1 \le k < \infty \tag{4*}$$

und[2])

$$|\xi_1 \xi_2 \ldots \xi_k| < 1 + k\beta \quad \text{für} \quad 1 \le k \le n. \tag{5}$$

Für die ersten Ungleichungen (4) *soll hier ein einfacherer Beweis als früher gegeben werden, der zugleich unter Berücksichtigung des Grades n zur genaueren Aussage*

$$|\xi_1 \xi_2 \ldots \xi_k| \le \sigma_k \alpha^k \left[1 - \left(\frac{k}{k+1}\right)^{n+1}\right]^{\frac{1}{2}} \quad \text{für} \quad 1 \le k \le n \tag{4**}$$

führt. Die zweiten Ungleichungen (5) *lassen sich zu den Abschätzungen*

$$|\xi_1 \xi_2 \ldots \xi_k| < \tau_k(\beta) \quad \text{für} \quad 1 \le k \le n \tag{5*}$$

[1]) Vgl. SPECHT, W.: Abschätzung der Wurzeln algebraischer Gleichungen. Math. Z. **52**, 310—321 (1949), Satz 4.

[2]) Vgl. SPECHT, W.: Zur Theorie der algebraischen Gleichungen. Jahresber. D.M.V. **48**, 142—145 (1938).

mit den gleichfalls vom Grade n unabhängigen Konstanten

$$(5^{**}) \qquad \begin{cases} \tau_k(\beta) = \left(\dfrac{(k-1)\beta^2 + \beta\sqrt{(k-1)^2\beta^2 + 4k + 2}}{2} \right)^{\frac{1}{2}} \times \\ \qquad \times \left(\dfrac{2k - (k-1)\beta^2 + \beta\sqrt{(k-1)^2\beta^2 + 4k}}{2k} \right)^{k/2} \end{cases}$$

verbessern. Ohne Einschränkung darf für das Weitere

$$\alpha > 0 \quad \text{und} \quad \beta > 0$$

vorausgesetzt werden.

Als gemeinsame Grundlage dient folgende Bemerkung[3]):

Mit der Norm

$$N = N(f) = (1 + |a_1|^2 + |a_2|^2 + \cdots + |a_n|)^{\frac{1}{2}}$$

des Polynoms $f(x)$ gilt

$$|\xi_1 \xi_2 \ldots \xi_k| \leq N \quad \text{für} \quad 1 \leq k \leq n.$$

Setzen wir demgemäß mit einer vorerst unbestimmten positiven Größe u

$$y = u\,x \quad \text{und} \quad g(y) = u^n f(x) = y^n + a_1 u\, y^{n-1} + a_2 u^2 y^{n-2} + \cdots + a_n u^n,$$

so gelten für die Nullstellen

$$\eta_\nu = u\,\xi_\nu \quad \text{für} \quad 1 \leq \nu \leq n$$

des Polynoms $g(y)$ die Ungleichungen

$$|\eta_1 \eta_2 \ldots \eta_k|^2 \leq 1 + |a_1 u|^2 + |a_2 u^2|^2 + \cdots + |a_n u^n|^2,$$

sodaß für die Nullstellen des Polynoms $f(x)$ mit einem beliebigen Wert $z = u^2$ folgt:

$$(6) \qquad |\xi_1 \xi_2 \ldots \xi_k|^2 \leq \frac{1 + |a_1|^2 z + |a_2|^2 z^2 + \cdots + |a_n|^2 z^n}{z^k} \quad \text{für} \quad 1 \leq k \leq n.$$

Unter der Voraussetzung

$$|a_\nu| \leq \alpha^\nu \quad \text{für} \quad 1 \leq \nu \leq n \quad \text{mit} \quad \alpha = \max_{1 \leq \nu \leq n} \sqrt[\nu]{|a_\nu|}$$

erhalten wir aus (6)

$$|\xi_1 \xi_2 \ldots \xi_k|^2 \leq \frac{1 + \alpha^2 z + \alpha^4 z^2 + \cdots + \alpha^{2n} z^n}{z^k}$$

und unter der Beschränkung

$$0 < \alpha^2 z = t < 1$$

die Ungleichung

$$(7) \qquad |\xi_1 \xi_2 \ldots \xi_k|^2 \leq \alpha^{2k} \frac{1 - t^{n+1}}{(1-t)\,t^k}$$

[3]) Vgl. a. a. O. [1]), Satz 1.

und ohne Berücksichtigung des Grades n des Polynoms $f(x)$ die Ungleichung

$$(7^*) \qquad |\xi_1 \xi_2 \dots \xi_k|^2 < \frac{\alpha^{2k}}{(1-t)\,t^k}.$$

Die Funktion

$$F(t) = (1-t)\,t^k$$

nimmt ihr Maximum an der Nullstelle $t_0 = \frac{k}{k+1}$ ihrer Ableitung

$$F'(t) = k\,t^{k-1} - (k+1)\,t^k$$

an; für die Stelle t_0 gilt

$$F(t_0) = (1-t_0)\,t_0^k = \left(1 - \frac{k}{k+1}\right)\left(\frac{k}{k+1}\right)^k = \frac{k^k}{(k+1)^{k+1}}.$$

Damit gewinnen wir in der Tat

$$|\xi_1 \xi_2 \dots \xi_k|^2 < k^{-k}(k+1)^{k+1}\alpha^{2k} \quad \text{für} \quad 1 \leq k \leq n,$$

wie in (4) behauptet worden war.

Bei Berücksichtigung des Grades n des Polynoms $f(x)$ entnimmt man der Ungleichung (7) für den gleichen Wert $t_0 = \frac{k}{k+1}$ des Parameters t die Abschätzung

$$|\xi_1 \xi_2 \dots \xi_k|^2 \leq k^{-k}(k+1)^{k+1}\left(1 - \left(\frac{k}{k+1}\right)^{n+1}\right)\alpha^{2k},$$

in Übereinstimmung mit der Ungleichung (4**).

Unter Verwendung des Parameterwertes

$$\alpha^2 z_0 = t_0 \quad \text{oder} \quad z_0 = \alpha^{-2}\frac{k}{k+1}$$

können wir bei der genaueren Festsetzung

$$a_\nu = \alpha^\nu \varepsilon_\nu \quad \text{mit} \quad |\varepsilon_\nu| \leq 1 \quad \text{und} \quad \alpha = \max\left|\sqrt[\nu]{a_\nu}\right| \quad \text{für} \quad 1 \leq \nu \leq n$$

die Ungleichung (6) auswerten zu der Abschätzung

$$|\xi_1 \xi_2 \dots \xi_k|^2 \leq$$

$$\leq \alpha^{2k}\left(\frac{k}{k+1}\right)^{-k}\left(1 + |\varepsilon_1|^2\,\frac{k}{k+1} + |\varepsilon_2|^2\left(\frac{k}{k+1}\right)^2 + \dots + |\varepsilon_n|^2\left(\frac{k}{k+1}\right)^n\right),$$

also

$$(8) \quad |\xi_1 \xi_2 \dots \xi_k| \leq \alpha^k \left[\frac{(k+1)^n + |\varepsilon_1|^2(k+1)^{n-1}k + |\varepsilon_2|^2(k+1)^{n-2}k^2 + \dots + |\varepsilon_n|^2 k^n}{(k+1)^n k^k}\right]^{\frac{1}{2}}.$$

Für die Nullstelle ξ_1 maximalen absoluten Betrages folgt hieraus insbesondere

$$(8^*) \qquad |\xi_1| \leq 2\alpha\left[\frac{2^n + |\varepsilon_1|^2 2^{n-1} + |\varepsilon_2|^2 2^{n-2} + \dots + |\varepsilon_n|^2}{2^{n+1}}\right] < 2\alpha.$$

Die aus der Ungleichung

$$(6) \qquad |\xi_1 \xi_2 \dots \xi_k|^2 \leqq \frac{1 + |a_1|^2 z + |a_2|^2 z^2 + \dots + |a_n|^2 z^n}{z^k} = \frac{g(z)}{z^k} = \Phi_k(z)$$

hervorgehende günstigste Schranke

$$|\xi_1 \xi_2 \dots \xi_k| \leqq \Phi_k^{\frac{1}{2}}(z^*)$$

liefert natürlich die (einzige) positive Nullstelle z^* der Ableitung

$$\Phi_k'(z) = \frac{z\, g'(z) - k\, g(z)}{z^{k+1}},$$

also der Gleichung

$$\varphi(z) = k + \sum_{\nu=1}^{} (k - \nu)\, |a_\nu|^2 z^\nu = 0.$$

Auf die Ungleichung (4) stützt sich auch die folgende Bemerkung über reelle Polynome

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n \quad \text{mit} \quad \alpha = \max_{1 \leq \nu \leq n} |\sqrt[\nu]{a_\nu}|.$$

Für jedes Paar $\omega, \bar{\omega}$ konjugierter imaginärer Nullstellen des reellen Polynoms $f(x)$ besteht die Ungleichung

$$|\omega \bar{\omega}| < \sigma_2 \alpha^2 \quad \text{oder} \quad |\omega| < \sigma_2^{\frac{1}{2}} \alpha.$$

Eine Nullstelle ξ_1 des reellen Polynoms $f(x)$, die dem Kreisring

$$\sigma_2^{\frac{1}{2}} \alpha \leqq |z| < \sigma_1 \alpha$$

der Zahlenebene angehört, ist demnach reell und durch diese Begrenzung eindeutig bestimmt.

Liegt dieser Sonderfall vor, so erfüllen alle Paare $\omega, \bar{\omega}$ konjugierter imaginärer Nullstellen die Ungleichung

$$\sigma_2^{\frac{1}{2}} \alpha |\omega \bar{\omega}| \leqq |\xi_1 \xi_2 \xi_3| < \sigma_3 \alpha^3 \quad \text{oder} \quad |\omega| < \sigma_3^{\frac{1}{2}} \sigma_2^{-\frac{1}{4}} \alpha.$$

Setzt man demgemäß

$$\tau_0 = \sigma_1 = 2, \quad \tau_1 = \sigma_2^{\frac{1}{2}} = 2^{-\frac{1}{2}} 3^{\frac{1}{4}} \sim 1{,}612, \quad \tau_2 = \sigma_3^{\frac{1}{2}} \sigma_2^{-\frac{1}{4}} = 2^{\frac{1}{4}} 3^{-\frac{1}{8}} \sim 1{,}382,$$

so gilt:

Ist $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n$ ein reelles Polynom mit der Schranke

$$\alpha = \max_{1 \leq \nu \leq n} |\sqrt[\nu]{a_\nu}|,$$

so liegen alle Nullstellen ξ des Polynoms im Kreisbereich

$$0 \leqq |z| < \tau_0 \alpha$$

und mit höchstens einer (reellen) Ausnahme ξ_1 im Kreisbereich

$$0 \leqq |z| < \tau_1 \alpha.$$

Liegt eine Nullstelle ξ_1 im Kreisbereich

$$\tau_1\alpha \leq |z| < \tau_0\alpha,$$

so liegen alle weiteren reellen bzw. imaginären Nullstellen im Kreisbereich

$$0 \leq |z| < \tau_1\alpha \quad \text{bzw.} \quad 0 \leq |z| < \tau_2\alpha.$$

Bei Verwendung der in (2.2) erklärten Größe β erhalten wir aus (6) die Ungleichung

$$|\xi_1 \xi_2 \dots \xi_k|^2 \leq \frac{1 - z + \beta^2 (z - z^{n+1})}{(1-z)\, z^k} \tag{9}$$

und ohne Berücksichtigung des Grades n des Polynoms $f(x)$ auch

$$|\xi_1 \xi_2 \dots \xi_k|^2 < \frac{1 + (\beta^2 - 1)\, z}{(1-z)\, z^k} = G(z). \tag{9*}$$

Um das Minimum der Funktion $G(z)$ im Intervall $0 < z < 1$ zu bestimmen, bilden wir mit der Abkürzung $\delta = \beta^2 - 1$ die Ableitung

$$G'(z) = \frac{(1-z)\,\delta z - (k - (k+1)\,z)\,(1 + \delta z)}{(1-z)^2\, z^{k+1}} = \frac{g(z)}{(1-z)^2\, z^{k+1}}$$

mit dem Polynom

$$g(z) = k\,\delta z^2 - \big((k-1)\,\delta - (k+1)\big)z - k,$$

das wegen

$$g(0) = -k; \quad g(1) = \delta + 1 = \beta^2 > 0$$

genau eine Nullstelle z_0 im Intervall $0 < z_0 < 1$ besitzt, nämlich

$$z_0 = \begin{cases} \dfrac{k}{k+1} & \text{für} \quad \beta = 1, \\ \dfrac{(k-1)\,\beta^2 - 2k + \beta \sqrt{(k-1)^2 \beta^2 + 4k}}{2(\beta^2 - 1)\, k} & \text{für} \quad \beta \neq 1. \end{cases}$$

Daraus folgt

$$G(z_0) = \frac{(k+1)^{k+1}}{k^k}$$

bzw.

$$G(z_0) = (\beta^2 - 1)^{\frac{(k-1)\beta + \sqrt{(k-1)^2\beta^2 + 4k}}{(k+1)\beta - \sqrt{(k-1)^2\beta^2 + 4k}}} \left(\frac{2(\beta^2 - 1)\, k}{(k-1)\beta^2 - 2k + \beta \sqrt{(k-1)^2 \beta^2 + 4k}} \right)^k.$$

Setzt man im Falle $\beta \neq 1$ abkürzend

$$R = \sqrt{(k-1)^2 \beta^2 + 4k},$$

so gewinnt man bei Berücksichtigung der Gleichungen

$$[(k+1)\beta - R]\,[(k+1)\beta + R] = 4k(\beta^2 - 1),$$

$$[(k-1)\beta + R]\,[(k+1)\beta + R] = 2k[(k-1)\beta^2 + 2 + \beta R],$$

$$[(k-1)\beta^2 - 2k + \beta R]\,[(k-1)\beta^2 - 2k - \beta R] = -4k^2(\beta^2 - 1)$$

die einfachere Gestalt

$$G(z_0) = \frac{(k-1)\beta^2 + \beta R + 2}{2}\left(\frac{2k - (k-1)\beta^2 + \beta R}{2k}\right)^k$$

und damit die Ungleichung

(10) $$|\xi_1 \xi_2 \dots \xi_k| < G^{\frac{1}{2}}(z_0) = \tau_k(\beta) \quad \text{für} \quad 1 \leqq k \leqq n$$

mit den in (5**) angegebenen Werten; sie ist übrigens auch im Falle $\beta = 1$ gültig.

Daß die Ungleichungen (10) die Abschätzungen (5) verbessern, geht aus den Beziehungen

(11.1) $$\tau_1(\beta) = 1 + \beta \quad \text{für} \quad 0 < \beta;$$

(11.2) $$\tau_k(\beta) < 1 + k\beta \quad \text{für} \quad 0 < \beta;\ 2 \leqq k < \infty$$

hervor. Zunächst stellen wir die Gleichung

$$\tau_1(\beta) = 1 + \beta$$

leicht fest, so daß weiterhin $k \geqq 2$ angenommen werden darf. Auf Grund der Minimaleigenschaft des Wertes z_0 bestehen für die Parameterwerte

$$0 < z_1 = \frac{k}{k+\beta} < 1 \quad \text{und} \quad 0 < z_2 = \frac{k}{k+1} < 1$$

die Beziehungen

(12) $$\tau_k^2(\beta) = G(z_0) \leqq G(z_1) = (1 + \beta k)\left(\frac{k+\beta}{k}\right)^k < (1 + \beta k)\, e^{\beta}$$

bzw.

(12*) $$\tau_k^2(\beta) = G(z_0) \leqq G(z_2) = (1 + \beta^2 k)\left(\frac{k+1}{k}\right)^k < (1 + \beta^2 k)\, e.$$

Im Falle $0 < \beta < 1$ gilt

$$0 < \frac{e^{\beta} - 1}{\beta} < e - 1 < 2 \leqq k, \quad \text{also} \quad e^{\beta} < 1 + \beta k$$

und damit nach (12)

$$\tau_k^2(\beta) < (1 + k\beta)\, e^{\beta} < (1 + k\beta)^2, \quad \text{also} \quad \tau_k(\beta) < 1 + k\beta.$$

Im Falle $1 \leqq \beta$ und $3 \leqq k$ entnehmen wir aus (12*)

$$\tau_k^2(\beta) < (1 + \beta^2 k)\, e < k + \beta^2 k^2 < (1 + \beta k)^2.$$

Im allein noch verbleibenden Falle $k = 2$ und $\beta \geqq 1$ entnehmen wir aus (12*) zunächst

$$\tau_2^2(\beta) < (1 + 2\beta^2)\left(\tfrac{3}{2}\right)^2 = \tfrac{9}{4} + \tfrac{9}{2}\beta^2.$$

Die Ungleichung

$$\tfrac{9}{4} + \tfrac{9}{2}\beta^2 \geqq (1 + 2\beta)^2 = 1 + 4\beta + 4\beta^2$$

besteht wegen $\beta \geqq 1$ nur im Falle

$$\beta \geqq 4 + \tfrac{3}{2}\sqrt{6} > 7.$$

Andererseits erhalten wir aus

$$\tau_2^2(\beta) = \left(\frac{\beta^2 + \beta\sqrt{\beta^2+8}+2}{2}\right)\left(\frac{4-\beta^2+\beta\sqrt{\beta^2+8}}{4}\right)^2$$

wegen

$$\sqrt{\beta^2+8} < \beta + \frac{4}{\beta}$$

die Abschätzung

$$\tau_2^2(\beta) < (\beta^2+3)\,4.$$

Die Ungleichung

$$(\beta^2+3)\,4 \geqq (1+2\beta)^2 = 1+4\beta+4\beta^2$$

besteht nur im Falle

$$12 \geqq 1+4\beta \quad \text{oder} \quad \beta \leq \frac{11}{4}.$$

Mithin gilt auch

$$\tau_2(\beta) < 1+2\beta \quad \text{für} \quad \beta \geqq 1.$$

Erlangen, Mathematisches Institut der Universität.

(Eingegangen am 3. Juli 1955.)

Pólya, G.
Math. Zeitschr. Bd. 63, S. 331—337 (1955)

On the characteristic frequencies of a symmetric membrane *).

Dedicated to the memory of I. Schur.

By
G. Pólya.

1. *Notation.* We consider a simply connected open domain $\mathfrak{D}$ in the z-plane, $z = x + iy$; we let $\mathfrak{C}$ denote the (sufficiently smooth) boundary curve of $\mathfrak{D}$. The function $u = u(x, y)$ is defined in $\mathfrak{D}$ and satisfies the differential equation

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \nu^2 u = 0 \quad \text{in } \mathfrak{D}. \tag{1.1}$$

We consider two, very different, boundary conditions:

$$u = 0 \quad \text{on } \mathfrak{C}, \tag{1.2}$$

$$\frac{\partial u}{\partial n} = 0 \quad \text{on } \mathfrak{C}; \tag{1.3}$$

n stands for the normal to $\mathfrak{C}$. In both cases, there exists an infinity of characteristic frequencies ν; let $\lambda_1, \lambda_2, \ldots$ denote the values of ν with the condition (1.2), and $\mu_1, \mu_2, \ldots$ with the condition (1.3);

$$0 < \lambda_1 < \lambda_2 \leqq \lambda_3 \leqq \cdots, \tag{1.4}$$

$$0 = \mu_1 < \mu_2 \leqq \mu_3 \leqq \cdots. \tag{1.5}$$

Let $\dot{r}$ denote the *maximum inner conformal radius of* $\mathfrak{D}$, defined as follows. We map the interior of $\mathfrak{D}$ conformally onto the interior of a circle so that the point a of $\mathfrak{D}$ corresponds to the center of the circle and the linear magnification at the point a is equal to 1; let the radius of the circle so obtained be r_a. The value of r_a varies with the point a, and $\dot{r}$ is the maximum of r_a.

We say that the domain $\mathfrak{D}$ possesses *symmetry of order* n if $\mathfrak{D}$ coincides with itself after a rotation through an angle $2\pi/n$ about a certain point O, called the center of symmetry if $n \geqq 2$. Any domain possesses symmetry of order 1, a square has symmetry of order 4, a circle symmetry of every order.

2. *Aim.* The products $\lambda_n \dot{r}$ and $\mu_n \dot{r}$ depend only on the shape of the domain $\mathfrak{D}$, not on its size. G. Szegö and the present author have shown that $\lambda_1 \dot{r}$ attains its maximum when $\mathfrak{D}$ becomes a circle [3, p. 97—98][1]). M. Schiffer and the present author have shown that, for any n,

$$\left(\frac{1}{\lambda_1^2} + \frac{1}{\lambda_2^2} + \cdots + \frac{1}{\lambda_n^2}\right)\frac{1}{\dot{r}^2}$$

*) Sponsored by the Office of Naval Research.

[1]) Numerals in square brackets refer to the Bibliography at the end of the paper.

attains its minimum when $\mathfrak{D}$ becomes a circle [2, p. 304—307; attention to the difference of notation]. It follows from a theorem recently proved by G. SZEGÖ that also $\mu_2 \dot{r}$ attains its maximum for the circle [4]. Yet, for higher values of n, we can not generally assert that $\lambda_n \dot{r}$ or $\mu_n \dot{r}$ attains its maximum for the circle. In fact, Table 1 shows that both assertions are wrong for $n = 5$.

If, however, we restrict the choice of $\mathfrak{D}$ and admit only convex domains with sufficiently high symmetry, both $\lambda_n \dot{r}$ and $\mu_n \dot{r}$ will be maximum for the circle. This is expressed more precisely by the following theorem.

Table 1.

n	$\lambda_n \dot{r}$		$\mu_n \dot{r}$	
	Circle	Square	Circle	Square
1	2.405	2.396	0.000	0.000
2	3.832	3.789	1.841	1.695
3	3.832	3.789	1.841	1.695
4	5.135	4.793	3.054	2.396
5	5.135	5.358	3.054	3.389

Table 2.

n	$2n+1$	$l(n)$	$m(n)$
1	3	3	3
2	5	6	6
3	7	10	8
4	9	15	12
5	11	19	17

There are two increasing functions $l(n)$ and $m(n)$ of the positive integer n, with the following property: If the domain $\mathfrak{D}$ is convex and possesses a symmetry of order not lower than $2n+1$ but is not a circle, each of the $l(n)+m(n)-1$ quantities

$$\lambda_1 \dot{r}, \lambda_2 \dot{r}, \ldots, \lambda_{l(n)} \dot{r}, \quad \mu_2 \dot{r}, \ldots, \mu_{m(n)} \dot{r}$$

belonging to $\mathfrak{D}$ will be inferior to the corresponding quantity belonging to a circle.

Table 2 contains a few values of $l(n)$ and $m(n)$.

As it can be seen from the full definition in Section 4(a)

$$l(n+1) - l(n) \geq 2, \quad m(n+1) - m(n) \geq 2. \tag{2.1}$$

For example, let us consider a square. It has symmetry of order 4, which is higher than 3. Now, as Table 2 shows, $l(1) = m(1) = 3$, and so our theorem asserts that each of the values

$$\lambda_1 \dot{r}, \lambda_2 \dot{r}, \lambda_3 \dot{r}, \mu_2 \dot{r}, \mu_3 \dot{r}$$

belonging to the square must be less than the corresponding value belonging to the circle; see Table 1. Yet for $\lambda_5 \dot{r}$ or $\mu_5 \dot{r}$ such an assertion is wrong, as Table 1 shows.

The principal aim of the present paper is to prove the theorem here formulated. I stated that part of the theorem that is concerned with λ_n some time ago [1]. Additional remarks are presented in Section 5.

3. *Lemma.* It is convenient to define the frequencies $\lambda_1, \lambda_2, \ldots, \mu_1, \mu_2, \ldots$ by their extremal properties which are connected with the RAYLEIGH ratio

$$R[f] = \frac{\iint |\operatorname{grad} f|^2 \, dx \, dy}{\iint f^2 \, dx \, dy} \,. \tag{3.1}$$

The function $f=f(z)$ can be considered also as a function of the two real variables x and y; f is defined in the domain $\mathfrak{D}$, which is also the domain of integration of both double integrals arising in (3.1); of course

$$|\operatorname{grad} f|^2 = f_x^2 + f_y^2.$$

The most convenient is, in our case as in many other cases, to use a lemma due to POINCARÉ [2, p. 275—278] which we formulate here in detail only for one of the two cases with which we are concerned.

Suppose that the functions $g_1, g_2, \ldots, g_l$, defined, realvalued, and sufficiently smooth in $\mathfrak{D}$ and on $\mathfrak{C}$, are linearly independent and that

$$g_1 = g_2 = \cdots = g_l = 0 \text{ on } \mathfrak{C}. \tag{3.2}$$

Suppose also that the quadratic forms $\Sigma\Sigma\, a_{ik} x_i x_k$ and $\Sigma\Sigma\, b_{ik} x_i x_k$, the latter of which is positive definite, are such that for all values of $x_1, x_2, \ldots, x_l$ (0, 0, …, 0, of course, excepted)

$$R[x_1 g_1 + x_2 g_2 + \cdots + x_l g_l] \leqq \frac{\Sigma\Sigma\, a_{ik} x_i x_k}{\Sigma\Sigma\, b_{ik} x_i x_k}. \tag{3.3}$$

Let the roots of the characteristic equation

$$\begin{vmatrix} a_{11} - x\, b_{11} & \ldots & a_{1l} - x\, b_{1l} \\ \cdots & \cdots & \cdots \\ a_{l1} - x\, b_{l1} & \ldots & a_{ll} - x\, b_{ll} \end{vmatrix} = 0 \tag{3.4}$$

be $x = \lambda_1'^2, \lambda_2'^2, \ldots, \lambda_l'^2$, increasingly ordered so that

$$0 < \lambda_1' \leqq \lambda_2' \leqq \cdots \leqq \lambda_l'. \tag{3.5}$$

Then

$$\lambda_1 \leqq \lambda_1', \quad \lambda_2 \leqq \lambda_2', \ldots, \lambda_l \leqq \lambda_l'. \tag{3.6}$$

It is convenient to call $g_1, \ldots, g_l$ the "trial functions". We shall need two corollaries of this lemma.

(a) *If the case of equality is excluded in* (3.3), *it is necessarily also excluded in each of the l resulting relations* (3.6). The proof given l. c. [2, p. 277] yields also this corollary.

(b) *If*

$$a_{ik} = \iint \operatorname{grad} g_i \cdot \operatorname{grad} g_k \, dx\, dy$$
$$b_{ik} = \iint g_i g_k \, dx\, dy$$

(so that the inequality (3.3) *becomes an equation) and the trial functions $g_1, g_2, \ldots, g_l$ coincide with the first l eigenfunctions of $\mathfrak{D}$, all the l inequalities* (3.6) *become equations.* Also this corollary is proved l. c. [2, p. 278].

4. *Proof.* It will be enough to prove what the theorem of Section 2 states about λ_n; the proof of the similar assertion dealing with μ_n is strictly parallel and presents no additional difficulty.

(a) The eigenfunctions of the equation (1.1) under the boundary condition (1.2) are well known when the domain is the unit circle. They are of the form

$$J_p(\lambda\varrho)\cos p\vartheta, \quad J_p(\lambda\varrho)\sin p\vartheta \tag{4.1}$$

where ϱ and ϑ are the polar coordinates of an arbitrary point ζ inside the unit circle; that is,

$$\zeta = \varrho e^{i\vartheta} \tag{4.2}$$

with $0 \leqq \varrho < 1$, $-\pi \leqq \vartheta \leqq \pi$. The corresponding characteristic frequency is λ, and p is an integer that we shall call the *type* of the eigenfunction. If the type is 0, only the first of the two expressions (4.1) is an eigenfunction, the second vanishes identically.

We define $l(n)$ as the greatest integer with the property that none of the eigenfunctions belonging to the characteristic frequencies

$$\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_{l(n)} \tag{4.3}$$

is of a type superior to n. We call the eigenfunctions corresponding to the frequencies (4.3)

$$\chi_1(\zeta), \chi_2(\zeta), \chi_3(\zeta), \ldots, \chi_{l(n)}(\zeta), \tag{4.4}$$

respectively.

(b) We consider the domain $\mathfrak{D}$ mentioned by our theorem. Thus $\mathfrak{D}$ is not a circle, but it is convex and symmetric of order q, where

$$q \geqq 2n+1. \tag{4.5}$$

The domain $\mathfrak{D}$ lies in the z-plane. Let the origin be the center of symmetry of $\mathfrak{D}$.

Let the power series

$$z = c_0\zeta + c_1\zeta^{q+1} + c_2\zeta^{2q+1} + \cdots \tag{4.6}$$

express the conformal mapping of the unit circle in the ζ-plane onto $\mathfrak{D}$ in the z-plane; (4.6) maps the center of the circle into the center of symmetry of $\mathfrak{D}$. Since $\mathfrak{D}$ is convex, we can assert [3, p. 22, 161—163] that

$$|c_0| = r. \tag{4.7}$$

(c) We wish to apply the lemma of Section 3. We construct the trial functions $g_k(z)$ by *transplanting* the eigenfunctions of the unit circle into $\mathfrak{D}$. That is, we define $g_k(z)$ by postulating that

$$g_k(z) = \chi_k(\zeta) \tag{4.8}$$

when z and ζ are connected by (4.6). Since $\chi_k(\zeta)$ vanishes on the boundary of the unit circle, $g_k(z)$ must vanish on the boundary of $\mathfrak{D}$, and so it fulfills the condition (3.2) of the lemma.

We set $l(n) = l$ and, in view of (4.8), we set

$$\begin{cases} f(z) = x_1 g_1(z) + \cdots + x_l g_l(z) \\ \quad = x_1\chi_1(\zeta) + \cdots + x_l\chi_l(\zeta) = \varphi(\zeta). \end{cases} \tag{4.9}$$

We transform the integrals in the numerator and denominator of the RAYLEIGH ratio $R[f(z)]$, see (3.1), by introducing the polar coordinates ϱ, ϑ in the ζ-plane instead of the rectangular coordinates x, y in the z-plane; we have to use (4.9), (4.6), and (4.2) for this purpose. Observing that the numerator of the RAYLEIGH ratio (the DIRICHLET integral) is a conformal invariant [3, p. 95], we obtain

$$R[f(z)] = \frac{\iint |\operatorname{grad} \varphi(\zeta)|^2 \varrho \, d\vartheta \, d\varrho}{\iint [\varphi(\zeta)]^2 \left|\frac{dz}{d\zeta}\right|^2 \varrho \, d\vartheta \, d\varrho}. \tag{4.10}$$

It is understood that for these double integrals (and for the other double integrals that will be considered in the present section) the domain of integration is the unit circle, so that ϱ and ϑ vary from 0 to 1, and from $-\pi$ to π, respectively.

Set

$$\left|\frac{dz}{d\zeta}\right|^2 = \frac{dz}{d\zeta}\,\overline{\frac{dz}{d\zeta}} = \sum_{\nu=0}^{\infty} (\nu q + 1)^2 |c_\nu|^2 \varrho^{2\nu q} + H(\zeta). \tag{4.11}$$

According to (4.6), $H(\zeta)$ is an absolutely convergent double infinite series consisting of terms of the form

$$C \varrho^{h'} e^{ih\vartheta} \quad \text{with} \quad |h| \geqq q \geqq 2n+1, \tag{4.12}$$

see (4.5); C is a constant, h' and h are integers, $h' > 0$. On the other hand, according to (4.9), the definition of $l = l(n)$, and (4.1), $[\varphi(\zeta)]^2$ is the sum of a finite number of terms which are all of the form

$$\psi(\varrho) e^{ik\vartheta} \quad \text{with} \quad |k| \leq 2n; \tag{4.13}$$

$\psi(\varrho)$ depends on ϱ alone (not on ϑ) and k is an integer. Integrating the product of the terms (4.12) and (4.13) with respect to ϑ from $-\pi$ to π, we get 0, and we conclude hence that

$$\iint [\varphi(\zeta)]^2 H(\zeta) \varrho \, d\vartheta \, d\varrho = 0. \tag{4.14}$$

It follows from (4.9), (4.10), (4.11), (4.14), and (4.7) that

$$\left\{ \begin{aligned} R[x_1 g_1 + x_2 + \cdots + x_l g_l] &= \frac{\iint |\operatorname{grad} \varphi(\zeta)|^2 \varrho \, d\vartheta \, d\varrho}{\iint [\varphi(\zeta)]^2 \sum_{\nu=0}^{\infty} (\nu q + 1)^2 |c_\nu|^2 \varrho^{2\nu q+1} \, d\vartheta \, d\varrho} < \\ &< \frac{\iint |\operatorname{grad} \varphi(\zeta)|^2 \varrho \, d\vartheta \, d\varrho}{\dot{r}^2 \iint [\varphi(\zeta)]^2 \varrho \, d\vartheta \, d\varrho}. \end{aligned} \right. \tag{4.15}$$

In fact, we can exclude the case of equality in the last step under (4.15), since $\mathfrak{D}$ is not a circle and so some of the coefficients $c_1, c_2, c_3, \ldots$ must be different from zero.

The last line of (4.15) is, by (4.9), the ratio of two quadratic forms in the variables $x_1, \ldots, x_l$. The roots of the corresponding characteristic equation are, as it is easily seen from Section 3 (b), $\lambda_1^{0\,2} \dot{r}^{-2}, \ldots, \lambda_l^{0\,2} \dot{r}^{-2}$ where $\lambda_1^0, \ldots, \lambda_l^0$

stand for the first l characteristic frequencies of the unit circle. It follows from (4.15), by virtue of the lemma of Section 3 and its corollary (a), that

$$\lambda_1 < \lambda_1^0 \dot{r}^{-1}, \ldots, \lambda_l < \lambda_l^0 \dot{r}^{-1}$$

which is the desired theorem.

5. *Additional remarks.* (a) *If the simply connected domain $\mathfrak{D}$ varies without any restriction, $\lambda_n \dot{r}$ possesses a finite upper bound that depends on n alone.*

This theorem, which I stated some time ago [*1*], can be proved by the method of Section 4. In fact, for the present purpose, we do not transplant all the successive eigenfunctions of the circle into $\mathfrak{D}$, as we did in Section 4(c), but only those of type 0; we use the terminology of Section 4(a). We obtain so easily the upper bounds, of which the first yields a "best" result [*3*, p. 97—98]:

$$\lambda_1 \dot{r} \leq 2.4048, \quad \lambda_2 \dot{r} \leq 5.5201, \quad \lambda_3 \dot{r} \leq 8.6537, \ldots^2).$$

The method of proof works also for the μ_n and yields the bounds:

$$\mu_2 \dot{r} \leq 3.8317, \quad \mu_3 \dot{r} \leq 7.0156, \quad \mu_4 \dot{r} \leq 10.1735, \ldots$$

Just the existence of a bound for $\mu_n \dot{r}$ follows from that for $\lambda_n \dot{r}$ since, as it is well known, $\mu_n < \lambda_n$.

(b) M. SCHIFFER found a very different method to prove the fact stated under (a). Indeed, if $\dot{r}$ is the maximum inner radius of the domain $\mathfrak{D}$, then $\mathfrak{D}$ contains, as is well known, a full circle of radius $\dot{r}/4$. Now the λ_n are monotonically decreasing domain functionals, and so each λ_n of $\mathfrak{D}$ is less than the corresponding λ_n of the circle with radius $\dot{r}/4$, which yields:

$$\lambda_1 \dot{r} \leq 9.619, \quad \lambda_2 \dot{r} \leq 15.328, \quad \lambda_3 \dot{r} \leq 15.328, \ldots$$

At the beginning, the bounds just obtained are higher than those obtained under (a), yet at the end, for sufficiently large n, the opposite is true.

(c) We do not know, for example, the least upper bound of $\lambda_2 \dot{r}$, or for which shape of $\mathfrak{D}$ this bound is attained or approximated. It may be worthwhile to mention that we can solve a similar problem.

Let A denote the area of $\mathfrak{D}$. Then

$$\lambda_2^2 A > 2j^2 \pi \tag{5.1}$$

where j, approximately 2.4048, is the first root of $J_0(x)$; the right hand side of (5.1) *is the greatest lower bound of the left hand side.*

This result is due to PETER SZEGÖ. It is based on the well known theorem, discovered by Lord RAYLEIGH and proved by G. FABER and E. KRAHN [*3*, p. VI, 191, 275],

$$\lambda_1^2 A \geq j^2 \pi. \tag{5.2}$$

[2]) Of course, the numerical values are only approximate and should be replaced by the appropriate zeros of the appropriate Bessel function.

We shall use (5.2) in its sharpest form: equality is attained only if $\mathfrak{D}$ is a circle.

We consider a more general situation: we assume that the nodal lines of the eigenfunction that corresponds to the characteristic frequency λ of $\mathfrak{D}$ dissect $\mathfrak{D}$ into s subdomains $\mathfrak{D}_1, \mathfrak{D}_2, \ldots, \mathfrak{D}_s$ of area $A_1, A_2, \ldots, A_s$, respectively; of course, $s \geqq 2$ and

$$A_1 + A_2 + \cdots + A_s = A. \tag{5.3}$$

The eigenfunction considered vanishes along the boundary of each of the subdomains $\mathfrak{D}_1, \mathfrak{D}_2, \ldots, \mathfrak{D}_s$, and so λ is a characteristic frequency of each. Applying (5.2) s times, we obtain

$$\lambda^2 A_1 \geqq j^2 \pi, \ldots, \lambda^2 A_s \geqq j^2 \pi. \tag{5.4}$$

Equality cannot be valid in each of the s relations (5.4): otherwise each of the s subdomains would be an open circular disk which obviously could not be fitted together into one *connected* open domain $\mathfrak{D}$. Hence, adding the inequalities (5.4) and using (5.3) we obtain

$$\lambda^2 A > s j^2 \pi \tag{5.5}$$

which for $s = 2$ yields the desired (5.1). In fact, only the eigenfunction corresponding to λ_1 is without nodal lines, and so for λ_2 we must have $s \geqq 2$. (Indeed, we have $s = 2$ for λ_2 by a theorem of COURANT.) This proof suggests also the shape of $\mathfrak{D}$ that renders the difference of the two sides of (5.1) infinitesimal: the union of two equal circles with given radius the common chord of which is of infinitesimal length.

Bibliography.

[1] PÓLYA, G.: Sur le rôle des domaines symétriques dans le calcul de certaines grandeurs physiques. Comptes Rendus Paris **235**, 1079—1081 (1952). — [2] PÓLYA, G., and M. SCHIFFER: Convexity of functionals by transplantation. J. Analyse Mathématique **3**, 245—345 (1954). — [3] PÓLYA, G., and G. SZEGÖ: Isoperimetric Inequalities. Princeton 1951. — [4] SZEGÖ, G.: Inequalities for certain eigenvalues of a membrane of given area. J. of Rational Mechanics and Analysis **3**, 343—356 (1954).

Department of Mathematics, Stanford University, Stanford, Cal. (U.S.A.).

(Eingegangen am 4. Juli 1955.)

LOEWNER, C.
Math. Zeitschr. Bd. 63, S. 338—340 (1955)

On totally positive matrices.

In memoriam ISSAI SCHUR.

By

CHARLES LOEWNER*).

A matrix $A = (a_{ij})$ is called totally positive if all its minors are non-negative. A product of two totally positive matrices is again totally positive. The totally positive square matrices of order n form therefore a semigroup S_n. The non-singular matrices of S_n represent then the elements of a subsemigroup s_n of the group of all real non-singular square matrices of order n[1]).

The semigroup s_n contains the identity matrix I. This fact allows the introduction of the concept of an infinitesimal element of s_n by the following definition adopted from the theory of Lie-groups: Let $U(t)$ be a differentiable matrix function of the real parameter t in an interval $0 \leqq t \leqq t_0$, representing for each t an element of s_n, and let $U(0) = I$. We call then the matrix $\left(\frac{dU(t)}{dt}\right)_{t=0}$ an infinitesimal element of s_n and the totality σ_n of all infinitesimal elements of s_n the infinitesimal semigroup of s_n.

Let now $\Omega(t)$ be a sectionwise continuous function of t $(0 \leqq t \leqq t_0)$ giving for each t an element of σ_n. The differential equation

$$\frac{dU(t)}{dt} = \Omega(t)\, U(t) \tag{1}$$

has a unique continuous solution satisfying the initial condition

$$U(0) = I. \tag{1'}$$

In the same way as in Lie-group theory one shows that $U(t_0)$ represents an element of s_n. It is called generated by the infinitessimal elements $\Omega(t)$ $(0 \leqq t \leqq t_0)$. In general, a semigroup cannot be completely recreated from its infinitesimal semigroup, even if the semigroup is connected. That this reconstruction is possible in case of our s_n is the essential content of this note. It may be considered as a grouptheoretical interpretation of a theorem by A. M. WHITNEY[2]).

*) This paper was written while the author was under contract with the Office of Scientific Research, Air Research and Development Command.

[1]) Regarding literature on totally positive matrices see e.g. I. J. SCHOENBERG: On smoothing operators and their generating function. Bull. Amer. Math. Soc. **50**, 199—230 (1953).

[2]) WHITNEY, A. M.: A reduction theorem for totally positive matrices. J. d'Analyse Math., Jerusalem **2**, 88—92 (1952).

We first determine the structure of σ_n by proving the

LEMMA. *A matrix $\Omega=(\omega_{ij})$ is an element of σ_n if and only if $\omega_{ij}=0$ for $|i-j|>1$ and all ω_{ij} $(|i-j|=1)$ are non-negative.*

PROOF. We use the above definition $\Omega=\left(\frac{dU(t)}{dt}\right)_{t=0}$ with $U(t)=(u_{ij}(t))$ representing for each t an element of s_n and $U(0)=I$. We have in particular $u_{ij}(t)\geq 0$ and $u_{ij}(0)=0$ for $i\neq j$. This leads to

$$\omega_{ij}\geq 0 \quad (i\neq j). \tag{2}$$

Consider next in case $n>2$ a second order minor

$$\begin{matrix} u_{kj}(t) & u_{kk}(t) \\ u_{ij}(t) & u_{ik}(t) \end{matrix} \qquad (i>k>j).$$

Since again it is non-negative and vanishes for $t=0$ its derivative at $t=0$ must be non-negative, i.e.

$$-\omega_{ij}\geq 0 \quad \text{for} \quad i-j>1. \tag{3'}$$

In the same way one proves that

$$-\omega_{ij}\geq 0 \quad \text{for} \quad j-i>1. \tag{3''}$$

By combining (3') and (3'') with (2) we see that the conditions of the lemma are necessary. In order to prove their sufficiency we start with the remark that σ_n forms a convex cone in the matrix space, i.e. that with two elements Ω_1 and Ω_2 of σ_n any linear combination $c_1\Omega_1+c_2\Omega_2$ with non-negative coefficients c_1 and c_2 belongs to σ_n. Indeed if $\Omega_1=\left(\frac{dU_1(t)}{dt}\right)_{t=0}$ and $\Omega_2=\left(\frac{dU_2(t)}{dt}\right)_{t=0}$, the matrices $U_1(t)$ and $U_2(t)$ all belonging to s_n and $U_1(0)=U_2(0)=I$, then $U(t)=U_1(c_1t)U_2(c_2t)$ also belongs to s_n and $U(0)=I$. Derivation at $t=0$ yields $\left(\frac{dU(t)}{dt}\right)_{t=0}=c_1\Omega_1+c_2\Omega_2$.

The preceding remark allows to consider only matrices Ω satisfying the condition of the lemma with only one non-zero element. If the latter is a diagonal element the matrices $e^{\Omega t}(t\geq 0)$ generated from the fixed Ω are diagonal matrices with positive diagonal elements and belong therefore to s_n. If the non-zero element is an $\omega_{ij}>0$ $(|i-j|=1)$ the matrices generated are

$$e^{\Omega t}=I+\omega_{ij}tE_{ij} \quad (t\geq 0), \tag{4}$$

E_{ij} being the matrix with all elements zero with the exception of a one at the crossing of the i-th row and the j-th column. But one verifies easily that the inequality $\omega_{ij}>0$ has the total positivity of the matrices (4) as consequence. This completes the proof of the lemma.

We now make use of the reduction theorem for totally positive matrices by A. M. WHITNEY[2]) which for non-singular square matrices of order n can be put into the form:

WHITNEY'S THEOREM. *Call* $I+\omega E_{ij}=F_{ij}(\omega)$. *Then every non-singular totally positive matrix* U *can be written as a product*

$$U = U_1 \cdot U_2 \dots U_{n-1} D V_1 \cdot V_2 \dots V_{n-1}, \tag{5}$$

where the U_i *and the* V_i, $i=1, 2, \dots, n-1$, *are of the form*

$$U_i = F_{n,n-1}(\omega^i_{n,n-1}) F_{n-1,n-2}(\omega^i_{n-1,n-2}) \dots F_{i+1,i}(\omega^i_{i+1,i}) \tag{5'}$$

$$V_i = F_{n-i,n-i+1}(\omega^i_{n-i,n-i+1}) F_{n-i+1,n-i+2}(\omega^i_{n-i+1,n-i+2}) \dots F_{n-1,n}(\omega^i_{n-1,n}) \tag{5''}$$

with all the ω*-s used non-negative, and* D *represents a diagonal matrix with positive diagonal elements.*

WHITNEY's theorem gives a parametric representation of the totally positive matrices.

According to our lemma each factor in (5'), (5'') and D can be generated from an element of σ_n and we have the

THEOREM. *Each element of* s_n *can be generated from infinitesimal elements of* σ_n.

Department of Mathematics, Stanford University, Stanford, Cal. (U.S.A.).

(Eingegangen am 19. Juli 1955.)

Motzkin, Th. S.
Math. Zeitschr. Bd. 63, S. 341—344 (1955)

A proof of Hilbert's Nullstellensatz.

In memoriam Issai Schur.

By
THEODORE S. MOTZKIN.

Hilbert's Nullstellensatz (1891) was reduced by RABINOWITSCH (1929) to Theorem 1 below. For the reduction and further references see ZARISKI [3] who gives two ideal-theoretic proofs. The proof of BRAUER [1] for the unreduced theorem is quite elementary. The following short and straightforward proof presupposes very little field theory and uses no ideals. It also furnishes bounds[1]), albeit weak, on the degrees (Theorems 2 and 3) and on the number of polynomials needed and thence yields another incompatibility criterion (Theorem 5). Exact bounds for the degree in a particular case and for the number of polynomials are given in Theorems 4, 6 and 7[2]).

Let K be a field, $x=(x_1, \ldots, x_n)$ an n-tuple of indeterminates, $K[x]$ the ring of polynomials and $K(x)$ the field of rational functions in x with coefficients in K. Let $\overline{K}$ be the algebraic closure of K.

Theorem 1. *If* $f_1, \ldots, f_r \in K[x]$ *are* $\neq 0, \ldots, 0$ *for every* $\xi=(\xi_1, \ldots, \xi_n)$, $\xi_1, \ldots, \xi_n \in \overline{K}$, *then* $\Sigma f_i g_i = 1$ *for some* $g_1, \ldots, g_r \in K[x]$.

Proof. $n=0$ is trivial; we use induction. Consider the f_i as polynomials in $K[x_2, \ldots, x_n]$ with coefficients in $K(x_1)$. By induction hypothesis[3]) we have $\Sigma f_i h_{i0} = a_0 \neq 0$, $h_{i0} \in K[x]$, $a_0 \in K[x_1]$. Let $a_0 = \Pi(x_1 - \xi_{1\lambda})$, $\xi_{1\lambda} \in \overline{K}$, and $K^* = K(\xi_{11}, \ldots, \xi_{1l})$. Again by induction hypothesis $\Sigma f_i(x_1 = \xi_{1\lambda})\, \varphi_{i\lambda} = 1$, $\varphi_{i\lambda} \in K^*[x_2, \ldots, x_n]$. Hence $\Sigma f_i \varphi_{i\lambda} - 1 = (x_1 - \xi_{1\lambda})\psi_\lambda$, $\psi_\lambda \in K^*[x]$. Now let $a_1 = a_0/(x_1 - \xi_{11})$, and $h_{i1} = \varphi_{i1}\, a_1 - h_{i0}\psi_1$; then $\Sigma f_i h_{i1} = a_1$. Removing the factors of a_0 one by one we end up with $\Sigma f_i h_{il} = 1$, $h_{il} \in K^*[x]$. If K^* is an extension of K with basis $b_1 = 1, \ldots, b_\varrho, \ldots$, and if $h_{il} = \Sigma g_{i\varrho} b_\varrho$, $g_{i\varrho} \in K[x]$, then $\Sigma f_i g_{i1} = 1$, Q.E.D.

Theorem 2. *If all* f_i *in Theorem* 1 *are of degree* $\leqq d$ *then the* g_i *may be chosen of degree* $\leqq d_n \leqq (d_{n-1} + d)\, \delta_{n-1} - d$, $d_0 = 0$, *where* δ_{n-1} *is defined in Theorem* 3[4]).

[1]) The existence of a bound (maybe not independent of the number of polynomials) is stated, e.g., in VAN DER WAERDEN [2], p. 5, exercise.

[2]) This work was sponsored (in part) by the National Bureau of Standards and by the Offices of Naval Research and of Ordnance Research and presented to the American Mathematical Society on November 27, 1954.

[3]) Any $\eta_2, \ldots, \eta_n \in \overline{K(x_1)}$ annihilating all f_i would for some $\xi_1 \in \overline{K}$ have values $\xi_2, \ldots, \xi_n \in \overline{K}$ with the same property. This is a special case of [2], p. 51, first theorem. [The latter also implies, applied to the residue field (p. 53), the existence of a zero for a maximal ideal and thus, by the maximal condition, p. 22, for every ideal $\neq 1$: an immediate proof using some ideal theory and field theory.]

[4]) The polynomial 0 is considered as of degree $-\infty$.

The *proof*[5]) follows the above steps. By assumption we have deg $h_{i0} \leqq \delta - d$, $l \leqq \delta$, where $\delta = \delta_{n-1}$ and deg denotes the degree. By induction hypothesis deg $\varphi_{i\lambda} \leqq d_{n-1}$ whence deg $\psi_\lambda \leqq d_{n-1} + d - 1$ (note that for additional indeterminates as in Theorem 3 and $d > 1$ the degrees of the numerators of $\varphi_{i\lambda}$ and ψ_λ might be greater or undefined). Further deg $a_1 \leqq \delta - 1$, deg $h_{i1} \leqq 2d_{n-1} + \delta - 1$, deg $h_{i\lambda} \leqq \delta - d + \lambda(d_{n-1} + d - 1)$, deg $g_{il} \leqq$ deg $h_{il} \leqq \delta (d_{n-1} + d) - d$, Q.E.D.

Let $y = (y_1, \ldots, y_m)$ be an m-tuple of additional indeterminates.

Theorem 3. *If* $f_1, \ldots, f_r \in K[x, y]$, *of degree* $\leqq d$, *are* $\not\equiv 0, \ldots, 0$ *for every* $\xi = (\xi_1, \ldots, \xi_n)$, $\xi_1, \ldots, \xi_n \in \overline{K(y)}$, *then* $\Sigma f_i g_i = a \not\equiv 0$ *for some* $g_1, \ldots, g_r \in K[x, y]$ *of degree* $\leqq \delta_n - d$ *and some* $a \in K[y]$ *of degree* $\leqq \delta_n \leqq \binom{n + d_n + d}{n+1} - \binom{n + d_n}{n+1}$, *where* d_n *is defined in Theorem* 2.

Note that the bounds given are not only independent of the individual f_i but also of r, m and K.

Proof. Let $f_i = \Sigma a_{ik} x^k$, $k = (k_1, \ldots, k_n)$, $0 \leqq k_\nu$, $\Sigma k_\nu \leqq d$, $x^k = \Pi x_\nu^{k_\nu}$, $a_{ik} \in K[y]$, deg $a_{ik} \leqq d - \Sigma k_\nu$. By Theorem 2 we have $\Sigma f_i g_{i1} = 1$ for some $g_{i1} = \Sigma b_{ik'} x^{k'}$, $b_{ik'} \in K(y)$, $0 \leqq k'_\nu$, $\Sigma k'_\nu \leqq d_n$. Now $\Sigma f_i g_{i1} = 1$ means $\sum_{i,k} a_{ik} b_{ik'} = 0 (k'' = k + k'$ fixed $\not\equiv 0$, $0 \leqq k''_\nu$, $\Sigma k''_\nu \leqq d + d_n), = 1 (k'' = 0)$. These are $\binom{n + d_n + d}{n}$ linear equations in the $b_{ik'}$. Let the rank of their coefficient matrix be c and choose in it c independent columns. Then the c corresponding $b_{ik'}$ are, after setting all other $b_{ik'} = 0$, uniquely determined from some c equations which include the inhomogeneous one, as quotients of the minors of order $c - 1$ belonging to that equation by the c-order determinant $a \not\equiv 0$. Since the degree of the $(k''; i, k')$-element of a is $\leqq d + \Sigma k'_\nu - \Sigma k''_\nu$ it follows that the degree of every term of a, as well as $d + \Sigma k'_\nu +$ the degree of every term of its $(0; i, k')$-minor, is $\leqq \gamma = \Sigma(d + \Sigma k'_\nu - \Sigma k''_\nu)$ where γ is independent of the term selected. Choosing a non-vanishing term we see that deg a and $d +$ deg $a b_{ik'} x^{k'}$ are $\leqq \gamma \leqq \Sigma \min(d + d_n - \Sigma k''_\nu, d) = \Sigma(d + d_n - \Sigma k''_\nu) - \Sigma \max(0, d_n - \Sigma k''_\nu) \leqq \binom{n + d_n + d}{n+1} - \binom{n + d_n}{n+1}$, Q.E.D.

For $d = 1$ Theorem 2 and 3 give $d_n = 0$, $\delta_n = 1$, the first of which expresses the duality theorem for linear equations. In this case the method of the proofs of Theorem 1 and 2 suffices to also obtain $\delta_n = 1$. For general d Theorem 2 and 3 imply $d_n \leqq d^{e_n} - d$, $\delta_n \leqq d^{n e_{n+1}}$ $\left(\text{by } \delta_n \leqq d\left(\binom{n + d_n + d}{n+1} - \binom{n + d_n + d - 1}{n+1}\right) = d\binom{n + d_n + d - 1}{n} \leqq d(d_n + d)^n\right)$, where $e_n = n!(1 + 1/1! + \cdots + 1/n!)$. Whereas perhaps $d_n \leqq n d / \ln(n+1)$ and $d_n \leqq n^{1 - 1/d}$ hold for $d \geqq n$ and $d \leqq n$, certainly $\delta_n > d^{n+1}$ as may be seen by considering general f_i for $r = n + 1$, $m = 1$. The bounds for d_n and δ_n drop somewhat by use of the following exact values for d_1 and δ_1.

Theorem 4. *In Theorem* 2 *and* 3, $d_1 = d - 1 (d > 0)$ *and* $\delta_1 = d^2$.

[5]) Simultaneous induction for Theorem 2 and 3.

Proof. For the proof of $d_1 = d-1$ we may suppose $a_{1d} \neq 0$. In $\Sigma f_i g_i = 1$ replace every g_i, $i>0$, by its remainder after division by f_1, while altering g_1 accordingly. This done, $\deg f_1 g_1 = \deg(1 - \sum_{i>1} f_i g_i) \leq 2d-1$, whence also $\deg g_1 \leq d-1$. Now $\delta_1 = d^2$ for $r=2$ by the reasoning in the proof of Theorem 3, with $\gamma = \Sigma d + \Sigma k' - \Sigma k'' = 2d^2 + 2\binom{d}{2} - \binom{2d}{2} = d^2$ (the matrix is the same as in the Sylvester resultant). For $r>2$ and infinite K, let $f_1^* = f_1$, $f_2^* = \Sigma z_i f_i$ with new indeterminates z_i and apply case $r=2$; then in $f_1^* g_1^* + f_2^* g_2^* = a^*$ replace the z_i by $\zeta_i \in K$ for which $a^*(\zeta_i) \neq 0$. To prove $\delta_1 = d^2$ for all K we use induction on r. Let be the greatest common divisor of $f_2, \ldots, f_r$ in $K[x, y]$ and hence also in $K(y)[x]$, and $d' = \deg f > 0$. Putting $f_i = \bar{f}_i f$, $i>1$, we have $\deg \bar{f}_i \leq d-d'$ and $\Sigma \bar{f}_i \bar{g}_i = \bar{a} \neq 0$ for some $\bar{g}_i \in K[x,y]$ of degree $\leq (d-d')^2 - (d-d')$ and some $\bar{a} \in K[y]$ of degree $\leq (d-d')^2$. On the other hand $f_1 \bar{g}_1 + fg = \bar{\bar{a}} \neq 0$ for some $\bar{g}_1$ and $g \in K[x, y]$, $\bar{\bar{a}} \in K[y]$, $\deg \bar{g}_1 \leq dd' - d$, $\deg g \leq dd' - d'$, $\deg \bar{\bar{a}} \leq dd'$; in fact $\gamma = dd'$ is seen to be the sum of the bounds for the degrees of the elements of the main diagonal of the Sylvester resultant of f_1 and f, after deducing $\deg_x \bar{g}_1 \leq d'-1$ and $\deg_x g \leq d-1$ as before. Hence $f_1 \bar{g}_1 \bar{a} + \Sigma f_i \bar{g}_i g = \bar{a}\bar{\bar{a}} \neq 0$ with $d + \deg \bar{g}_1 \bar{a}$, $d + \deg \bar{g}_i g$, $\deg \bar{a}\bar{\bar{a}}$ all $\leq dd' + (d-d')^2 \leq d^2$.

A polynomial h of degree $d+d'$ shall be called an *annihilator* of a polynomial f of degree d if $f(x_1^{-1}, \ldots, x_n^{-1})h$ contains no terms $\Pi x_\nu^{k_\nu}$, $k_\nu \geq 0$, $\Sigma k_\nu \leq d'$. If h has a non-vanishing constant term h is a *proper annihilator.*

Theorem 5. *The polynomials $f_1, \ldots, f_r \in K[x]$ of degree d have a common zero $\xi_1, \ldots, \xi_n \in \bar{K}$ if and only if they have a common proper annihilator $h \in K[x]$ of degree $d + d_n$, where d_n is defined in Theorem 2.*

Proof. The linear equations for b_{ik}, in the proof of Theorem 3 are, by duality, insolvable if and only if the equations $\sum_{k'' \geq k'} c_{k''} a_{i\,k''-k'} = 0$, $c_0 = 1$ for $c_{k''}$ are solvable. But this is tantamount to saying that $h = \Sigma c_{k''} x^{k''}$ is a proper annihilator of degree $d + d_n$ of every f_i.

The proof of Theorem 3 shows that no more than $\binom{n+d_n+d}{n}$ polynomials g_i are needed in Theorem 1 to 4. An improvement on this is obtained directly as follows.

Theorem 6. *In Theorem 1 to 4, all g_i but $\binom{n+d}{n}$ may be chosen as 0.*

Proof. The Theorem asserts that a smallest insolvable system of polynomial equations $f_i = 0$ has at most $r_0 = \binom{n+d}{n}$ members. Suppose it had $r > r_0$ members. Because of the minimality there exist points (n-tuples) $P_i = (\xi_{i1}, \ldots, \xi_{in})$, $\xi_{iv} \in \bar{K}$ such that $f_i(P_k) = 0$ for $i \neq k$. Since the f_i have r_0 coefficients one, say f_1, would be a linear combination of the others, whence $f_1(P_1) = 0$, against the insolvability supposition.

By the *Helly dimension* of a family of point sets we shall mean $r_0 - 1$, where r_0 is the smallest positive integer such that any subfamily with void

intersection must in turn contain a subfamily of $\leqq r_0$ sets with void intersection. (One of the "Helly theorems" states that the family of compact convex sets in n-space has Helly dimension n.) Using the basis theorem ([2], p. 20), the proof of Theorem 6 implies:

Theorem 7. *The Helly dimension of the family of hypersurfaces of degree d in affine or projective n-space is $\leqq$ its linear dimension* $r_0 - 1 = \binom{n+d}{n} - 1$.

In real or complex space, or any space over a field of infinite degree of transcendency, the hypersurfaces through $r_0 - 1$ from among r_0 general points will not have any point in common, whence r_0 points with this property can be found in every space over an infinite field, and the above Helly dimension is thus in these spaces exactly $r_0 - 1$.

References.

[1] BRAUER, R.: A note on Hilbert's Nullstellensatz. Bull. Amer. Math. Soc. **54**, 894—896 (1948). — [2] VAN DER WAERDEN, B. L.: Modern Algebra, vol. 2. New York 1950. — [3] ZARISKI, O.: A new proof of Hilbert's Nullstellensatz. Bull. Amer. Math. Soc. **53**, 362—368 (1947).

Added in proof. An ideal-theoretic proof of Theorem 1 is due to ANCOCHEA, G.: Sobre el "Nullstellensatz" de Hilbert. Ann. Mat. Pura Appl. (4) **29**, 31—34 (1949). A bound for d_n can be derived from HERMANN, G.: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. **95**, 736—788 (1926).

University of California, Los Angeles 24 (U.S.A.).

(Eingegangen am 26. Juli 1955).

Ergebnisse der exakten Naturwissenschaften

Herausgegeben von **S. Flügge** und **F. Trendelenburg**, unter Mitwirkung von W. Bothe und F. Hund.

Im Juli 1955 erschien:

Achtundzwanzigster Band: Mit 268 Abbildungen. III, 483 Seiten Gr.-8°. 1955. DM 79.80; Ganzleinen DM 83.—

Inhaltsübersicht: **Erzeugung und Anwendung von Röntgenblitzen.** Von W. Schaaffs, Berlin-Siemensstadt. — **Ergebnisse der Experimente mit künstlichen π-Mesonen.** Von H. Thurn, Frankenthal, Pfalz. — **Theoretische Behandlung von Problemen der Mesonenphysik.** Von S. Flügge, Marburg/Lahn. — **The spectroscopy of nuclear gamma-rays by direct crystal diffraction methods.** By J. W. M. DuMond, Pasadena, Cal., USA. — **Bedeutung von Korpuskularbestrahlung für die Eigenschaften von Festkörpern.** Von K. Lintner und E. Schmid, Wien. — **Technik und Anwendung der Kernemulsionen.** Von M. Teucher, Bern. — Inhalt der Bände 11—28. — Namen- und Sachverzeichnis.

Siebenundzwanzigster Band: Mit 271 Abbildungen. III, 421 Seiten Gr.-8°. 1953. DM 66.—, Ganzleinen DM 69.—

Inhaltsverzeichnis: **Theorie des rein elektrischen Durchschlags fester Isolatoren.** Von W. Franz, Münster (Westf.). — **Der Leitungsmechanismus in homöopolaren Halbleitern.** Von O. Madelung, Erlangen. — **Die Energieschemata der leichten Atomkerne. II. Teil: Die Energieschemata der Kerne ^{20}F bis ^{36}Cl.** Von U. Cappeller, Marburg/Lahn. — **Präparative Methoden der Elektronenmikroskopie und ihre Ergebnisse.** Von H. König, Darmstadt. — **Impulsverstärker und Impulsspektrographen.** Von E. Baldinger und W. Haeberli, Basel. — **Feldemission.** Von E. W. Müller, State College, Pa., USA. — **Szintillationszähler.** Von A. Krebs, Fort Knox, Kentucky, USA. — Inhalt der Bände 11—27. — Namen- und Sachverzeichnis.

Sechsundzwanzigster Band: Mit 110 Abbildungen. III, 439 Seiten Gr.-8°. 1952. DM 66.—; Ganzleinen DM 69.—

Elektromagnetische Wellenleiter. Von R. Honerjäger, Frankfurt a. M. — **Thermodynamisch-phänomenologische Theorie der irreversiblen Prozesse.** Von R. Haase, Marburg a. d. Lahn. — **Das Zwei-Nucleonen-Problem.** Von S. Flügge, Marburg a. d. Lahn. — **Das Schalenmodell des Atomkerns.** Von O. Haxel, J. H. D. Jensen, Heidelberg, und H. E. Suess, Chicago. — **Feldmechanik des Elektrons und der Elementarteilchen.** Von H. Hönl, Freiburg i. Br. — **Die Theorie des Kristallwachstums.** Von O. Knacke und I. N. Stranski, Berlin-Charlottenburg. — Inhalt der Bände 11—26. — Namen- und Sachverzeichnis.

SPRINGER-VERLAG / BERLIN · GÖTTINGEN · HEIDELBERG

Projektive Ebenen

Von Dr. **Günter Pickert,** apl. Professor der Mathematik an der Universität Tübingen. (Die Grundlehren der mathematischen Wissenschaften, Bd. LXXX.) Mit 60 Abbildungen. VIII, 343 Seiten Gr.-8°. 1955.

DM 44.80; Ganzleinen DM 48.60

Inhaltsübersicht: Erläuterungen. — **Grundbegriffe:** Inzidenzstrukturen. Projektive und affine Ebenen. Freie Erweiterungen. Schließungssätze. Koordinateneinführung in affinen Ebenen. Koordinaten in der dualen Ebene. — **Gewebe:** Darstellung von 3-Geweben mittels Loops. Isotopie. Die Bedingungen von Reidemeister, Bol und Thomsen. Darstellung von 4-Geweben mittels Doppel-Loops. — **Der Satz von Desargues:** Zentrale Kollineationen. Der Satz von Desargues. Die Ausartungen des Desarguesschen Satzes. Cartesische Gruppen und Quasikörper. Sonderfälle des Desarguesschen Satzes als Ternärkörpereigenschaften. — **Desarguessche Ebenen:** Kollineationen und homogene Koordinaten. Doppelverhältnisse. Quasiperspektivitäten. Der Satz vom Viereckschnitt. — **Der Satz von Pappos:** Mit dem Satz von Pappos gleichwertige Aussagen. Weitere Herleitungen des Desarguesschen Satzes aus dem Satz von Pappos. Homogenität einer projektiven Ebene. Ausartungen des Satzes von Pappos. — **Alternativkörper:** Definitionen und Rechenregeln. Alternativkörper als Algebra über dem Zentrum. Quadratische Algebren. Alternativkörper der Charakteristik 2. Rechtsalternativkörper. — **Moufang-Ebenen:** Moufang-Ebenen und Alternativkörper. Der Satz vom vollständigen Viereck. Die Kollineationsgruppe. — **Translationsebenen:** Darstellung durch Kongruenzen. Der Kern einer Translationsebene. Die Kollineationsgruppe. Translationsebenen der Charakteristik $\neq 2$. Translationsebenen über assoziativen Quasikörpern. — **Angeordnete Ebenen:** Anordnungen, Zwischen- und Trennbeziehungen. Angeordnete affine und projektive Ebenen. Einfluß der Anordnung auf die Koordinatenbereiche. Archimedische Anordnung. Ordnungsfunktionen. — **Topologische Ebenen:** Topologie und Ternärkörper. Angeordnete topologische Ebenen. — **Möbius-Netze:** Möbius-Netze und dreifache Ausartung des Desarguesschen Satzes. Schliessungssätze vom Rang 8. — **Endliche Ebenen:** Einordnung unter allgemeinere kombinatorische Begriffe. Punkteanzahl. Vollständige Vierecke mit kollinearen Diagonalpunkten. Desarguessche und zyklische Ebenen. Kollineationen. — **Anhang.** Kennzeichnung der Desarguesschen Ebenen als Untergruppenmengen. Beweis des Desarguesschen Satzes in einer projektiven Ebene mit genau 8 Punkten auf jeder Geraden. Ergänzendes über offene Inzidenzstrukturen. Vereinfachter Beweis des Hauptsatzes über Alternativkörper. Verzeichnis der Formelnummern. — Zeichenzusammenstellung. — Literatur und Sachverzeichnis.

SPRINGER-VERLAG / BERLIN · GÖTTINGEN · HEIDELBERG

Diesem Heft liegt ein Prospekt des Springer-Verlages, Berlin - Göttingen - Heidelberg, und ein Prospekt des Springer-Verlages, Wien, bei.

Springer-Verlag, Berlin · Göttingen · Heidelberg. — Druck der Universitätsdruckerei H. Stürtz AG., Würzburg.
Printed in Germany.